Survey of secure multipath routing protocols for WSNs

Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Mat Kiah, Ismail Ahmedy

Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya (UM), Kuala Lumpur 50603, Malaysia

Department of Web Technology, Faculty of Computer Science and Information Technology, University of Tun Hussein Onn (UTHM), Johor 86400, Malaysia

Journal of Network and Computer Applications

Abstract

In sensing data to the base station, wireless sensor networks (WSNs) face some security challenges since such networks impose resource constraints that need to be addressed by the routing mechanism. This paper surveys, explores, and informs researchers regarding the landscape of multipath routing by providing the motivation behind multipath routing deployment. Subsequently, this paper analyzes the security requirements and common attacks in wireless sensor networks. Also, we provide a classification of secure multipath routing protocols on the basis of nature of defense against the WSN attacks. According to the classification, we investigate the existing secure multipath routing protocols within the WSN domain by discussing their strengths and limitations. A comparative study of the suggested classification is presented based upon the multipath technique, additional security infrastructure, security requirements, corresponding attacks, and efficiency analysis in pursuit of effective secure routing in wireless sensor networks.

Contents

1. Introduction ................................................................. 124
2. Related work ............................................................. 124
3. Multipath routing in WSNs ........................................... 125
   3.1. The motivation for multipath routing ......................... 126
4. Analyses of security requirements for WSN .................. 127
5. Analyses of common attacks on WSNs ......................... 128
6. Secure multipath routing protocols .............................. 129
   6.1. The needs of security mechanisms in multipath routing 130
   6.2. The efficiency of secure multipath routing ............... 130
   6.3. The proposed classification ................................... 130
   6.4. The tolerant-based approach ................................. 131
      6.4.1. Hybrid-SPREAD ........................................ 131
      6.4.2. INSENS ............................................... 131
      6.4.3. Enhanced INSENS ................................... 132
      6.4.4. MVP .................................................. 134
      6.4.5. SEIF .................................................. 134
   6.5. The prevention-based approach ............................... 135
      6.5.1. SEEM .................................................. 135
      6.5.2. HSNRP ............................................... 136
      6.5.3. STAPLE ............................................... 138
      6.5.4. EENDMRP ........................................... 139

* Corresponding author at: Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya (UM), Kuala Lumpur 50603 Malaysia. Tel.: +60 1977771712.
E-mail address: shazanamdzin@gmail.com (S. Md Zin).

http://dx.doi.org/10.1016/j.jnca.2015.04.018
1084-8045/© 2015 Elsevier Ltd. All rights reserved.
1. Introduction

In recent years, there has been a huge interest in wireless sensor networks (WSNs) (Rawat et al., 2014). With the advancement in technology, many real applications have been deployed and new application areas have rapidly emerged. The sensor networks are composed of numerous numbers of resource constrained sensor nodes depending on the application, with a few base stations acting as a gateway to the outside network, such as the Internet. Wireless sensor networks have a wide range of applications such as military (Pathan et al., 2006), environmental (Sann and Minn, 2011), and other commercial applications. For instance, the WSN technology can be used to detect the position of incoming attacks in military applications. Moreover, sensor networks can be greatly beneficial for the environment to locate forest fires (Hefeeda and Bagheri, 2007) or to observe animal habits such as ant colonies (Alrajeh et al., 2013a). In healthcare applications (Al Ameen et al., 2010), the nodes are responsible for collecting patients’ physiological data and recording their periodic medical assessments. For commercial domain, wireless sensor networks can be deployed for indoor surveillance (Barati et al., 2008) and temperature regulation (Baghyalakshmi et al., 2011) in offices.

Unlike wired networks, routing in WSNs poses more challenges due to the unique characteristics of sensor nodes, such as them being prone to failures due to harsh deployment environments (Jing et al., 2013). Moreover, with the absence of fixed infrastructure, such nodes have to be autonomous and self-organizing within the network area (Lin et al., 2012b). All nodes in a sensor network communicate with each other via a wireless basis, which results to topology changes. Therefore, various attacks can leads to many security problems. For instance, the adversary has the ability to compromise a sensor node, eavesdrop on data transmission, inject false messages, and waste network resources (Yick et al., 2008). Hence, security provisioning for such networks is crucial to route data from source to the destination (Yun et al., 2008). However, there are constraints in incorporating security into a wireless sensor network (WSN) such as limitations in energy, computation, processing, memory, and communication capabilities (Brandl et al., 2009). Therefore, designing a secure protocol requires consideration of such limitations and achieving acceptable performance levels to meet the needs of specific applications. Since security remains a fundamental factor in data communication (Abduvaliyev et al., 2013), many routing protocols have been proposed, such as routing using the multipath mechanism.

The multipath routing technique is widely used to prolong the network lifespan (Nasser and Chen, 2007a) and be responsible for Quality-of-Service (QoS) provisioning (Huang and Fang, 2008) in wireless sensor network applications. Instead of single path, the data are routed through two or more paths, and therefore the multipath mechanism is considered to be more fault tolerant than the conventional single path approach (Alrajeh et al., 2013a). Multipath routing protects data security in WSNs against attacks by reducing the chance of a packet being modified or dropped by a malicious sensor node (Kohno et al., 2012). Moreover, lightweight security mechanism can be adapted to the multipath routing technique to further enhance the security of transmission by mitigating the impact of network attacks in WSNs (Khalil et al., 2010).

As discussed earlier, security provisioning for data communication is challenging in wireless sensor networks. Surveys by (Ehsan and Hamdadoi, 2011; Stavrou and Pitsillides, 2010) show that secure routing is an open issue for WSNs which motivates us to make an effort in this domain. This paper reviews the state-of-the-art for secure multipath routing in WSNs. We discuss the motivation behind the development of multipath routing, security requirements, and attacks on WSN. Besides providing readers with a landscape of multipath routing in WSN, the main purpose of this work is to focus on the needs of security mechanism support in multipath routing, discuss the efficiency of secure multipath approaches, as well as classifying the secure multipath routing on the basis of the nature of defense in responding to network attacks on WSNs. Further, we critically analyze the existing works in this research area. Also, we provide related figures associated with each protocol discussed in this survey. Moreover, the proposed matrix based upon the classification is presented in terms of the multipath technique, security mechanism support, security requirements, corresponding attacks, and efficiency with respect to secure multipath routing protocols in WSNs.

The remainder of the paper is structured as follows. In Section 2, the related work is briefly reviewed. Section 3 deals with the landscape of multipath routing in WSNs. In Section 4 and Section 5, the security requirements and common attacks on WSNs are discussed, respectively. Section 6 presents the security mechanism support, discusses the efficiency analysis in multipath routing, proposes a classification for secure multipath routing, and analyses the selected protocols based upon the classification. Section 7 summarizes the discussions. Finally, Section 8 provides conclusions derived from this survey. Table 1 shows the list of acronyms used in the paper.

2. Related work

The different requirements from various applications reflect the different performance focuses in routing protocol development (Al-Obaisat and Braun, 2007). Thus, many routing protocols have been proposed based upon the application motivations. Moreover, due to the importance of routing protocols, there is a set of literature reviewing the routing techniques of WSNs from various perspectives. Most of the surveys in the literature have focused on reviewing the different routing schemes for WSNs without considering security (Akkaya and Younis, 2005; Raghunandan and Lakshmi, 2011; Vick et al., 2008). Additionally, there are some researchers focused on a survey
of security issues who identify relevant open problems for future research, including the work of (Yong et al., 2006) and (Yun et al., 2008). In addition, another study on the important factors to secure routing protocols in sensor networks is presented by (Nikjoo et al., 2007). Other research work (Ozdemir and Xiao, 2009) has analyzed the relationship between security and data aggregation processes in WSNs. The work in (Sen, 2009) deals with security constraints and other security issues in WSNs such as the security mechanisms for WSNs. The survey proposed in (Sharma and Jena, 2011) focused on analyzing and comparing secure hierarchical routing protocols based on various criteria. Following the trends, (Schaffer et al., 2012) review the state-of-the-art of clustering protocols in WSNs with special emphasis on security and reliability issues.

Moreover, the work in (Alwan and Agarwal, 2009) focuses on a particular design component or a specific type of multipath objective, targeted to provide a reliable routing in WSNs. They classified the fault tolerant routing protocols into two classes, retransmission and replication based. The performance of those protocols is analyzed on the basis of performance metrics including energy consumption, memory usage and so on. The study in (Sha et al., 2013) reviewed the state-of-the-art of proposed multipath routing protocols for WSNs, which are classified into three categories: infrastructure, non-infrastructure, and coding based. For each category, they studied the design of protocols, analyzed the tradeoff of each design, and overviewed several representative protocols. Also, they discussed a summary of design goals, challenges, and evaluation metrics for multipath routing protocols in resource constrained systems. However, they did not consider security in their survey. Work in (Modirkhazeni et al., 2010) focused on security concerns and presented a matrix that analyzed the security factor provided by the secure multipath routing protocols in WSNs. In addition, the survey proposed in (Stavrou and Pitsillides, 2010) conducted another survey on the current state-of-the-art of secure multipath routing protocols in WSNs, classified the protocols in categories according to their security-related operational objectives, defined a new threat model in the routing procedure, and identified open research issues in the area. Therefore, we limit our coverage in this paper to the multipath schemes by discussing the state-of-the-art for secure multipath routing, outlining the motivation behind the development of multipath schemes, addressing the security requirements, and emphasizing the common attacks in wireless sensor networks. Also, this survey is distinguished from the existing works in the following ways:

(a) we focus on the needs of security mechanism support and the efficiency in multipath routing,
(b) we classify the secure multipath routing on the basis of nature of defense in responding to WSN attacks and investigate their protocol operation, benefits, and limitations according to the classification,
(c) we provide related figures for each protocol which is important to understand the protocols, and
(d) we propose a matrix based upon the classification in terms of the multipath technique, security mechanism support, security requirements, corresponding attacks, and efficiency analysis with respect to secure multipath routing protocols in WSNs.

3. Multipath routing in WSNs

The sensor network is typically deployed to monitor environmental and critical applications for some specific purpose such as
to detect temperature changes and battlefield surveillance (Ali and Fisal, 2008). In densely deployed WSNs, routing is crucial to send data between sensor nodes and the base station (BS). For instance, if two nodes are not within the transmission range of each other, the intermediate nodes are responsible for routing the data for communication between the two nodes. There are two types of routing techniques, unipath and multipath routing. The unipath or single path routing is simple since the route between the source and the destination nodes can be established in a specific period of time. Moreover, it is scalable because, even if the network scales from ten nodes up to thousand nodes, the complexity and the approach to discover the path remains the same. However, the single path routing is inadequate to effectively support the requirements of natural limitations imposed on sensor nodes. In this kind of routing, the route discovery process is performed with minimum computational and resource utilization. Therefore, the stringent capability of this approach highly decreases the achievable network throughput. Furthermore, the flexibility against node or link failure is low which also reduces the entire network performance in time critical applications. If the active path fails to transmit data packets due to limited battery power of the sensor nodes, high dynamics of wireless links, or physical interferences, constructing a new path to continue data transmission processes may cause extra overheads and latency. While considering the characteristics of WSNs, single path routing is inefficient to meet the performance demands of various applications due to the following reasons (Sha et al., 2013):

i. In data routing, the possibility for the source node to select the intermediate nodes from the same part of the network redundantly is high, which results in energy depletion of those sensor nodes and network partitions, thus shortens the lifetime of WSNs.

ii. The failure of a single node or path will disrupt the data flow from source to destination due to resource constraints, unreliable wireless communication, or dynamic topology in sensor networks. Once a node fails, it is unable to forward data packets within the particular network area. Similarly, when a link error occurs during packet transmission, no retransmission is performed for the same packet. Thus, if any failure occurs in single path routing, it cannot successfully deliver sensed data to the sink.

iii. The lack of enough paths contributes to significantly minimum security since the node compromise is persistent and the broadcast nature of communication makes information more vulnerable to different types of attacks in WSNs. If a single node is compromised, all the packets relayed by that node are considered compromised. The presence of a malicious node on the path can manipulate and corrupt the data without catching the attention of the sink node.

iv. Exchanging messages in single path routing leads to the problems of holes and network congestion since the data load are not shared among available paths.

v. Single path routing is incapable of supporting scalable sensor networks due to the significant delay in bypassing the failure nodes. The process of constructing a new path may decrease the network performances.

Therefore, to cope with the limitations of single path routing techniques, the multipath routing approach constructs a certain number of paths for data transmission from individual sensor nodes towards the destination as alternative paths in case the primary path malfunctions or is used for fault tolerance purposes. Moreover, the discovered paths can be utilized concurrently to provide adequate network resources in intensive traffic conditions (Radi et al., 2012). In multipath routing, if a small number of nodes or paths are compromised, the message as a whole is not affected by the malicious intent. Hence, the concept of multiple paths can be applied in two different ways either to use them alternately by using the primary path first (i.e., when the primary one fails, switch to the secondary one) or to use the multiple paths simultaneously (Lou and Kwon, 2006). Because of the nature of multipath routing that establishes more than one path, this type of routing can address the reliability, security, and energy efficiency issues of unipath routing protocols. Also, many multipath routing protocols have been proposed in the literature of the WSN research area. Multipath routing can be divided into two types, disjoint multipath and braided multipath. In disjoint multipath, a number of alternate paths are node disjointed between each other, which mean that the alternate routes are not node disjointed. Hence, the failure of a link only affects a single path (Li et al., 2013). Meanwhile, braided multipath are partially disjoint from each other (i.e., routes are partially overlapped) and not completely node disjoint. In particular, the alternative paths may join the primary path partially such that the primary and alternative paths are braided with nodes overlapping with each other (Zhang et al., 2010). Moreover, the focus has been on delivering packets along randomly disjoint multipath routes, since they do not have a fixed candidate route for selection (Tao et al., 2010). Therefore, it is possible to ensure that adversaries cannot know the routes, even if they obtain the routing algorithms in advance (Anfeng et al., 2012).

In the sensor networks, multipath transmissions are needed especially when the probability of being compromised by adversaries is high. This mechanism calls for sending k number of messages instead of one (Nikjoo et al., 2007).

Due to the limited range of wireless transmissions, it is necessary for sensor nodes to perform multipath routing in forwarding a packet to its destination, usually the base station. In addition, most previous works on multipath sensor network routing focus on energy efficiency (Yahya and Ben-Othman, 2009b), reliability (Guimin Huang et al., 2013), or Quality-of-Service (QoS) (Yahya and Ben-Othman, 2009a) as their design goals and assume a secure and trusted environment where all nodes cooperate without the existence of attackers. Hence, to deal with this kind of limitation, much attention has been given to multipath routing protocols in the field of secure routing since they are mostly preserving against adversary attacks on WSNs (Xiao and Chen, 2010). The optimal path between the pair of source and destination is selected by the routing protocols to satisfy the important selection metrics such as energy and bandwidth. The security criteria can be included on the path selection by considering the next hop behavior. Therefore, the routing protocols should take into consideration the important metrics such as minimum hop, minimum transmission cost, and high residual energy to route the data (Erdene-Ochir et al., 2010). In multipath routing, more than single paths are established to forward a packet to destination, thus the communication is increased in comparison to the single path approach which results in better network throughput (Stavrou and Pitsillides, 2010). This section presents the primary motivations behind using the multipath routing approach in wireless sensor networks.

3.1. The motivation for multipath routing

As mentioned above, the multipath routing technique has demonstrated its efficiency in improving wireless sensor networks’ performance against the single path routing. In conventional networks, (e.g., the Internet), the multipath mechanism has been utilized to offer load balancing and reliability of data delivery (Nasser and Chen, 2007b). In these approaches, multiple copies of data are sent along different paths, allowing for resilience to failure of a certain number of nodes or paths. Thus, multipath...
routing could be an effective solution to satisfy the requirements of routing protocols. Instead of transferring multiple copies of data, only a single optimal path is used between a pair of source and destination at any time whilst the remaining paths are maintained as the back-up routes. In a sensor network, multipath routing is developed according to primary motivations such as energy consumption, reliability and fault tolerance, load balancing, QoS improvement, and security (Fig. 1). Also, these motivations reflect to the performance benefits of multipath routing technique in WSNs. The details of each motivation is described as follows:

1. **Energy consumption**: The sensor nodes depend on the embedded batteries to perform their task. If a node is terminated due to low power, it may result in network partitioning. Since WSNs are deployed in harsh environments, a consistent energy supply or recharging facility is impractical. The single path routing schemes may not be optimal to maximize the network lifetime and connectivity. Thus, distributing the network traffic across multiple paths can preserve the energy consumption among the sensor nodes (Boulfekhar and Benmohammed, 2013). In this case, a set of paths are selected and established by means of a certain probability. The value of the probability depends on how low the energy consumption of each path can be achieved. By having paths chosen at different times, the energy of any single path will not deplete quickly and the energy cost overhead for data retransmissions is minimized (Ke and Li-Ming, 2010). In addition, by distributing the workload to multiple paths, the lifespan of the WSN will be expanded and congestion can be reduced under heavy traffic (Li et al., 2013).

2. **Reliability and fault tolerance**: Multipath routing is considered an effective mechanism in providing better resilience to various faults in sensor networks (Al-Hamadi and Ing-Ray, 2013). Also, the multipath routing technique is capable to smooth the traffic congestion and improving data delivery (Al-Hamadi and Chen, 2013). An improved reliability and fault tolerance can be achieved by sending more data than necessary along the multiple paths, which the reconstruction of the original information can tolerate up to a certain level of path failure or packet loss (Zhang and Yu, 2008). In the fault tolerance domain, whenever a sensor node fails to forward its data to the sinks, it can benefit from the availability of alternative paths to salvage its data packets from node or link failures. Therefore, since an alternative path is available from a target area towards the sink node, data forwarding can be continued without any interruption.

3. **Load balancing and bandwidth aggregation**: Due to the resource limitations of sensor nodes, intensive traffic loads in high-data rate applications are prone to congestion, which decreases the network performance. Hence, the multipath approach can benefit from the high density of WSNs to increase network throughput by employing more network resources. Furthermore, multipath routing can provide reasonable bandwidth requirements of different applications and reduce the probability of network congestion through splitting network traffic over multiple paths. Node disjoint multiple paths are selected for data transmission to spread the load among different nodes to provide an effective load sharing mechanism among the multiple paths in the WSNs (Sangeetha and Yuvaraju, 2012). Traffic congestion may decrease channel usage and cause the packet loss rate to increase that leads to packet drop and increased packet delay. Hence, network congestion can be slightly decreased by applying the general multipath schemes of WSNs (Li et al., 2013).

4. **QoS improvement**: The existing multipath schemes have demonstrated the effectiveness of traffic distribution over multipath to fulfill QoS requirements (e.g., network throughput, end-to-end delay, and data delivery ratio) in WSNs (Radi et al., 2012). The discovered multipath with various characteristics can be utilized to distribute network traffic based on the QoS demands of the application for which the multipath routing protocol has been designed. Many applications including intruder tracking, healthcare, and forest-fire monitoring are extremely time critical. Therefore, any physical events must be reported within a certain timestamp to ensure an inflexible deadline. In the case of path failures, multipath approaches can preserve the QoS demands of the intended application via disseminating network traffic to another active path. Therefore, multipath routing protocols provide an effective solution to satisfy the resource constraints and to meet the required QoS in the WSNs.

5. **Security**: The broadcast communication nature of WSNs is often susceptible to physical attacks (Di Pietro et al., 2014). Most of the sensor networks are developed for mission critical applications (i.e., military surveillance) and thus, security considerations are highly necessary. Since the sensor nodes are resource constrained (e.g., limited storage), heavyweight security mechanisms are impractical to embed in the sensor routing (Gaurav et al., 2012). Furthermore, most sensor nodes are not tamper resistant, and as a consequence the attacker can extract sensitive data from the nodes or configure a few nodes to launch malicious activities (Alrajeh et al., 2013a). By using multipath, alternative paths are constructed for each data transmission to overcome such attacks. Hence, the concept of multipath can be adapted to achieve better protection against intruders, enhance the security of transmitted data, and reduce the end-to-end delay (Khiani et al., 2014). Also, if a small number of paths are compromised, it will not affect the data message of the alternative routes entirely, only the failure of links might significantly impact the transmission performance (Li et al., 2013). Therefore, it is desirable to design an effective multipath routing scheme with consideration of the security motivation to balance the network performance and secure data communication in WSNs.

In this paper, with respect to paper length limit, we only present the secure multipath routing protocols. To focus on the main viewpoint of security, we discuss in the next section two-dimensions of security issues, which deliberate on security requirements and WSN attacks.

### 4. Analyses of security requirements for WSN

In most WSN applications, security becomes a fundamental concern in designing a secure routing protocol and also a highly significant requirement.
demanded property since all assets have to be protected from unauthorized intent (Md Zin et al., 2014; Simplicio et al., 2013). Compromising the routing operation can affect the whole network service. Therefore, security requirements support has to be considered in the development of WSN routing to evaluate the acceptance and use of sensor network in various applications. Since the nodes are small in size and low in cost, the nodes are not considered tamper-resistant. For instance, attackers with physical access to the node can extract sensitive data (e.g., keys) from the node relatively easily. Also, attackers can turn the normal node into a malicious one by uploading a malicious node into it. In contrast, the BS is assumed to be tamper-resistant and trustworthy. Also, it has much greater capabilities since it may have laptop capabilities and can dissipate the energy in a timely manner (Ismail and Sanavullah, 2008).

Throughout the literature, researchers have proposed appropriate security mechanisms including the multipath routing technique in order to address such requirements. The security goals in sensor network routing require confidentiality, authentication, integrity, and availability. Those security requirements should be performed by a secure routing protocol. However these features are application specific and it is unlikely that a universal secure routing algorithm that can fit all circumstances can be designed. Current routing protocols suffer from different types of security vulnerabilities such as malicious nodes injecting spoofed information, resulting in routing inconsistency, and susceptibility to replay attacks (Khiani et al., 2014). In multipath routing, the adversary may capture nodes to initiate malicious activities on the active paths. The objective of security services in WSNs is to protect the routing information and node resources from attacks. Hence, to minimize the vulnerabilities of multipath routing in WSNs, the following security requirements should be taken into account:

1. **Confidentiality:** In many mission-critical applications, key distribution is used to communicate highly sensitive data (Guermazi and Abid, 2011). Therefore it is extremely important to build a secure channel in a wireless sensor network. Confidentiality should be provided to ensure the routing data are well protected against unauthorized recipients. Moreover, it is essential to maintain the secrecy of important data transmitted between sensor nodes (Yun et al., 2008). This means that the routed data should be kept secret until it has reached the destination.

2. **Authentication:** Most applications in WSNs require data authentication such as for civilian applications (Misra and Dias Thomasinious, 2010). Since sensor networks communicate through wireless media, authentication is essential to enable sensor nodes to detect malicious packets (Shi and Perrig, 2004). Authentication allows the node to verify the original source of the packet, ensure the identity of the sender, and verify the network participants. Furthermore, such requirements are vital to ensure that false data are not injected in the network.

3. **Integrity:** Since attackers have great capabilities to alter or modify important data in the forwarded packets, integrity indicates the capability of a WSN to validate that a data message sent from one node to another are delivered without any alteration or modification by malicious intent. Sensitive applications such as healthcare monitoring rely on the integrity of the data in order to function properly. Inaccurate data will affect the decision-making and will lead to erroneous performance. The integrity requirement can be ensured by the use of security mechanisms such as cryptographic hash functions, which require obtaining a fingerprint for each digital message (Diop et al., 2013).

4. **Availability:** A single point of failure will greatly threatens the availability of the network. Therefore, to provide availability, the connectivity service offered by the WSNs should be well-functioning throughout its lifetime (Modirkhazeni et al., 2010). Loss of availability may have a major impact on the network itself. For instance, loss of availability in home sensor systems may cause failure of the alarm system and open a back door for burglar invasion. A number of attacks can compromise the availability of the sensor network. Moreover, such a requirement is important to ensure that the network is capable of providing services even in the presence of node or link failures and attackers.

Thus, in order to provide security in wireless sensor network routing, the consideration of fundamental security requirements in future protocol designs is essential. Some systems may satisfy one or more of the security requirements depend on the application (El-Semary and Abdel-Azim, 2013). Therefore, the implementation of such security requirements is imperative to thwart and defend the most common attacks against WSNs effectively. To further highlight these matters, the next section outlines the attacks on WSN routing.

### 5. Analyses of common attacks on WSNs

Securing WSNs becomes a crucial task due to their vulnerabilities to a wide range of network attacks. However, most of the existing works in WSNs are designed without considering the security aspects (Elshekaniki et al., 2008; Pal et al., 2010). Consequently, these protocols are subject to various potential threats associated with the network layer of ad hoc networks. For instance, in multipath routing, they are focused on attacking the limited energy of sensor nodes. The work in (Martins and Guyennet, 2010) has distinguished between passive and active attacks. The passive attack is aimed at obtaining transmitted data and is able to perform monitoring or eavesdropping. However, attacks in this category are unable to perform modification of data. Meanwhile, an active attack has the ability to manipulate the data such as to modify or delete it. Further, the study in (El-Semary and Abdel-Azim, 2013) defines categorization of attacks on WSNs routing protocols into: (i) attacks on information in transit, (ii) node replication attack, (iii) Denial-of-Service (DoS) attack, and (iv) routing attacks. We note that attacks on wireless sensor networks are not limited to simply DoS attacks, but encompass a variety of techniques including attacks on the routing protocols, the node compromised, and physical security attacks on the node. Identifying the possible threats and attacks on sensor networks will help in designing secure routing protocols (Abd-El-Barr et al., 2005). Following this section, we focus on the most common attacks on wireless sensor networks. In particular, it is easy to eavesdrop or cause network layer attacks which fall into one of the following categories:

1. **Spoofing, altering, and replaying routing information:** These attacks are targeted to influence routing information whilst it is being exchanged in the network. The disruption caused by spoofed, altered, or replayed routing information includes the creation of loops in routing, attracting, or repelling network traffic from select nodes, partitioning the network, creating false error, and increasing the end-to-end delay (Yong et al., 2006).

2. **Selective forwarding attack:** Packet forwarding is a basic task in routing operation. In this kind of attack, the malicious node forwards only chosen packets and simply drops others. The malicious activity has to be included in the path of the data flow to mount selective forwarding. In such cases, all the packets are dropped from the routing path (Du and Lin,
The impact of selective forwarding becomes crucial when these malicious nodes are closer to the BS. Therefore, many intermediate nodes route message via these malicious nodes. As a consequence, they affect the purpose of mission-critical applications such as military surveillance and smoke detection.

3. Sinkhole attack: The principle of sinkhole attack is that the malicious node tries to attract surrounding nodes with respect to the routing algorithm. This goal can be achieved by spoofing the route advertisement or by providing a high-quality path towards BS. The compromised nodes drop the data packets and refuse to forward them to the next hop which prevents the BS from receiving complete and correct sensing data (Roy et al., 2008). Consequently, surrounding nodes will choose the compromised node as the next node to route their data. Therefore, the malicious intent has the ability to modify the traffic and perform traffic analysis.

4. Wormhole attack: In a wormhole attack, two misbehavior nodes are connected to tunnel the data message over a low-latency channel between two distant networks and replay them. This link may be established either by a single node forwarding messages between two adjacent which are non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The message, which is supposed to traverse multiple nodes, traverses only a single path more quickly. The time of the delivery is important for the routing scheme, especially if the influenced message contains mission-critical routing information. Such an attack has a severe impact on routing protocols since the colluding nodes use a different communication channel to route packets (Khan and Javed, 2008). For instance, a wormhole is created between the BS and a node at the opposite side of the network, thus instead of multiple hops the node appears to be only a single hop from the BS.

5. Sybil attack: The Sybil attack occurs when a malicious node illegitimately presents multiple identities and advertises multiple identities to the rest of the network (Khalil et al., 2010), which can cause mischief in the network service. By presenting multiple identities, it can report false data to the sink node and the malicious node can claim to participate in the network, and thus the legitimate nodes are left with a minor chance to transmit. Protocol schemes that are easily affected include distributed storage, fault tolerant techniques, and network topology maintenance. For instance, a distributed storage scheme may rely on three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved while they have not in reality. Hence, a Sybil attack is difficult to detect and inflicts a significant impact on the routing process.

6. HELLO flood attack: To create a network, nodes announce themselves to their neighbors by broadcasting HELLO packets. With the intent to reach their neighbor, these nodes will send their messages beyond their radio range. Nodes receiving such packets conclude that the broadcasting node is their neighbor and within the same radio range. A device such as a laptop class attacker can use a powerful signal transmitter to send HELLO packets to compromise every node in the network and attract a large area of nodes in sending discovery packets (Halim and Islam, 2012). If the attacker broadcasts packets to the BS using the path used by the malicious node, all of these nodes will attempt transmission to the attacking node and subsequently their packets will be out of radio range. Figure 2 shows an example of this attack.

These security attacks initiate serious routing malfunctions in the underlying network. Some attacks are less severe while some are more severe. For instance, selective forwarding attacks drop certain packets and forward the rest to the next hop, whereas sinkhole attacks drop all the packets without forwarding them, and thus create a DoS circumstance that is difficult to confront. These network layer security attacks can be handled through the development of appropriate secure routing protocols. The use of wireless communication makes the sensor networks more prone to security threats ranging from passive eavesdropping to active interference. Without proper security provisioning, sensor nodes are easily captured, compromised, and altered by the malicious nodes. Therefore, the next section discusses the landscape of secure multipath routing with security mechanism support proposed by sensor network routing protocols.

6. Secure multipath routing protocols

Data routing from source to destination is one of the essential operations in WSN. Although many routing protocols have been proposed in this particular network, only a few of them consider the problem of security and most of them have been developed without any security consideration such as Directed Diffusion (Intanagonwiwat et al., 2003), Simple Least-Time Energy-Efficient Routing Protocol with One-Level Data Aggregation (LEO) (Misra and Dias Thomasinous, 2010), and Data Aggregation Ant Colony Algorithm (DAACA) (Lin et al., 2012a). In addition, most of the existing protocols are either application specific or lacking security mechanisms (Alrajeh et al., 2013b). Therefore, several routing protocols are proposed for sensor networks to ensure secure...
transmission of data in WSN (Altisen et al., 2013, Pathan and Hong, 2008). As mentioned in the previous section, the multipath routing scheme is recognized as one of the effective ways to overcome sensor network attacks. Hence, this section focuses on selected secure multipath routing protocols that have been proposed for WSNs. Also, other security mechanism supports have been adopted to enhance the security features of multipath routing protocols in sensor networks.

6.1. The needs of security mechanisms in multipath routing

It is inevitable that secure data transmission from source to destination nodes requires some sort of security mechanism. The normal trend of sensor network design is that they have little external security features, which increases the vulnerability of the devices and poses tougher security challenges (Al Ameen et al., 2010). Thus, the multipath routing technique is somewhat insufficient in defending certain types of WSN attacks. For instance, a Sybil attack can be launched to degrade multipath routing performance (Deng et al., 2006). Hence, sensor networks should consider the integration of multipath and additional security mechanism support to enhance the ability of the routing framework to reduce the impact of attacks. In some cases, the security mechanism support is adopted to mitigate the process of excluding the intruder from the entire network which means that it is imperative to act as a second layer of defense to counter specific security threat (Alrajeh et al., 2013b). Such solutions to counter the WSN attacks that threaten wireless sensor networks need to consider the specificities of the particular networks. For instance, researchers have to find lightweight countermeasures that allow securing the network whilst consuming as little energy as possible and these remedies can be adapted to low computing power. Besides multipath, most research into WSN security has focused on cryptography, key management, intrusion detection, broadcast authentication, secure routing, or trust management (Zahariandis et al., 2010; Rawat et al., 2014). Moreover, security mechanisms in sensor networks should deal with compromised nodes, such as detecting compromised nodes or revoking their cryptographic keys network-wide. In addition, key management schemes in sensor networks have the ability to exclude compromised nodes from the whole network by the revocation of the entire key rings of the compromised nodes (Lee and Choi, 2006). Also, a security mechanism is needed in order to provide integrity, authenticity, and confidentiality for the sensed data.

6.2. The efficiency of secure multipath routing

A huge number of researchers are working on secured and efficient routing protocols. Security is also marked equally to efficiency, such as the lifetime of the network (Kumar and Jena, 2010). Apart from the related issues regarding security, efficiency is another imperative issue that should be scrutinized in order to establish the performance of secure multipath routing protocols in sensor networks. Therefore, in this survey, we overlaid these two issues. Providing efficiency is a challenging task in any multipath routing scheme (e.g., path finding capability) (Lou and Kwon, 2006). Such protocols need to be measured in terms of efficiency to evaluate the performance within the particular network; for instance the data transmission capability and determining the productivity of routing protocols. Earlier studies in the field of sensor networks have focused on the efficiency and effectiveness of data routing (Du and Lin, 2005). Therefore, efficiency is vital to explain the factors that affect the operation of a protocol including energy, time, or cost. In addition, it can also be used for the specific purpose of delivering the capacity of sensor applications in particular, in order to effectively achieve certain results with reduced waste and expense. The efficiency of the secure routing protocols, such as estimation of the additional overhead, can be assessed through exhaustive simulations using the appropriate simulation platform. Most of the protocols have performed measurable concepts, which are quantitatively determined by the ratio of output to input. Therefore, in order to design a good protocol for wireless sensor networks, it is imperative to understand the parameters that are relevant to the sensor applications. While there are many ways in which the properties of sensor network protocols can be evaluated, most of the protocols discussed in this survey demonstrate the competence in performance in terms of the following:

1. Energy Consumption: A secure routing protocol for sensor network should be energy efficient which can rely on low energy consumption to lengthen the network lifespan. For instance, a clustering mechanism provides low latency and is also useful to preserve energy consumption (Gengsheng et al., 2009). It is inefficient for a routing protocol to utilize a large amount of energy whilst maintaining a quality connection that allows communication between the nodes. As the property of sensor nodes, it is unfeasible to replace node batteries, as they are deployed only once. In certain conditions, such as a harsh deployment environment, the sensors are unreachable. For instance, in wireless underground sensor networks, some sensor nodes are deployed only for sensing the soil (Gulhane and Mahajan, 2014).

2. Delay: The sensor routing protocol should achieve better performance in terms of end-to-end delay with respect to the expanded scalability of the network size. In addition, data from sensor networks are typically time sensitive, thus it is vital for the data to be received at the intended destination in a timely manner. Therefore, the sink node can make intelligent decisions based on the node's available resources, hop count to the source, and delay to extend the network lifetime in order to provide fault-tolerance, to achieve the desired network state, and to meet the different application requirements (Alwan and Agarwal, 2010). Also, the duration to set up each phase of the routing protocol should be as least as likely to avoid latency.

3. Overhead: The routing overhead is controlled by different parameters used in the proposed algorithm such as computation cost. For instance, excessive route request data that are received on each sensor node may increase the overhead in terms of the processing and communication costs as well as the memory storage. Moreover, the changes in network topology can introduce significant overheads, especially for highly utilized networks. In terms of constructing a new path for data transmission, this process may lead to extra overhead due to the failure of alternatives paths.

4. Reliability: Reliability reflects the success of the end-to-end data delivery ratio. It has been an important factor in WSNs, since the nodes are prone to failure and the wireless transmission between the nodes is susceptible to many kinds of interferences (Lou and Kwon, 2006). Reliability requirements need to be supported, meaning that the ability of the network for packet delivery has to be restored in case of attack compromise (Stavrou and Pitsillides, 2012).

Therefore, the efficiency issue is significant in terms of dealing with security in order to strengthen the security analysis of this survey.

6.3. The proposed classification

In this section, we focus on the selected secure multipath routing protocols in WSNs, which are developed mainly using multipath, and some of them are developed with the integration
of other security mechanisms. We classify the selected secure multipath routing protocols into three main categories namely detection-based, prevention-based, and hybrid approaches (Fig. 3). The rationale behind the proposed classification is to categorize the protocols on the basis of nature of defense in responding to network attacks on WSNs. All categories aim to counter specific types of WSN attacks and therefore minimize the impairment of the network. The major concern of the protocols within the first category is to reduce the impact of intruder to disrupt the network function. The basic idea of prevention-based approach is to stop the deceptive attacks launched by attackers using the aid of additional security mechanism. The mixed-mode approach can be the integration of tolerant, detection, and prevention support in their routing mechanism in order to limit the capability of malicious node, to detect the misbehaving nodes, and adapt to the network changes as well as to avoid the potential attacks from interfering the sensor network.

Therefore, the proposed classification is important to analyze the security performance of the existing routing frameworks based upon their ability to respond to typical WSN attacks. This section summarizes the existing approaches for secure multipath routing protocols based upon the proposed classification to further analyze their benefits, limitations, and efficiency analysis. In order to address the main points of concern, seventeen secure multipath schemes have been selected which have focused on providing security in their routing performance.

6.4. The tolerant-based approach

The tolerant-based approach provides robustness in the multipath scheme where the compromise of a small number of paths will maintain the network connectivity to function correctly because of the existence of alternative routes. In some cases, it requires multiple copies of data messages to be sent to the intended destination. Thus, it is imperative to limit the damage caused by an intruder who has compromised the deployed sensor nodes. Hence, this section discusses the secure multipath routing with tolerant-based approach.

6.4.1. Hybrid-SPREAD

The design of H-SPREAD (Hybrid-Secure Protocol for REliAble Data delivery) routing protocol aims to tackle security and reliability issues (Lou and Kwon, 2006). The conceptual framework of H-SPREAD is adopted from the distributed N-to-1 multipath discovery protocol, which is able to discover multiple node-disjoint paths to the BS simultaneously. Further, the hybrid multipath data collection scheme is proposed to tolerate failures and compromised nodes. The threshold secret sharing scheme is constructed to split the information in traversing the multiple paths. H-SPREAD combined hybrid multipath data dispersion and secret sharing increases security. Figure 4 presents the multipath discovery procedure in H-SPREAD which includes: (a) branch aware flooding and (b) multipath extension flooding. In the first phase, while each node in the sensor network has a primary path to the BS by following its tree links up, a link between two nodes that belong to two different branches will provide each node an alternate disjoint path to the BS through the other. However, the ability to find extra paths by the branch-aware flooding is limited to nodes that have immediate neighbors. In the second phase, the flooding technique is used to find more node-disjoint paths at each sensor node with the cost of some extra message exchanges. Therefore, the routing mechanism is designed to maximize the number of disjoint paths at each node by further propagating the alternate paths found at the phase one across the multiple branches.

The security and efficiency performance of H-SPREAD is evaluated in terms of data delivery, failure tolerances, and compromised nodes in a probabilistic manner. The results show that the proposed hybrid multipath scheme is more resilient to tolerating node or link failures and a collusive attack of the compromised nodes. Also, H-SPREAD is resilient against node capture, thus the compromise of a small number of paths will not affect the transmitted data in unaffected paths in the present of a malicious node. In terms of reliability, H-SPREAD uses an active per-hop packet salvaging strategy to have a greater chance of delivering packets to the destination. The proposed N-to-1 multipath discovery protocol takes advantage of flooding and finds multiple node-disjoint paths from every sensor node to the common sink node simultaneously to enhance the effectiveness of path finding. If a node detects that a packet is unreachable to the next hop, it forwards the packet via the back-up paths to avoid packet dropping. However, the effectiveness of the N-to-1 multipath routing algorithm can be decreased by wireless interference. As a consequence, high packet loss ratio due to disruption can reduce the probability of successful data delivery on the sink node. Also, the extended branch aware flooding contributes to excessive overhead in the network performance. Moreover, due to the absence of any authentication mechanism, H-SPREAD only improves the reliability and security of data transmission in the network, without enhancing the security of the individual nodes.

6.4.2. INSENS

INSENS (Intrusion-tolerant routing protocol for wireless Sensor NetworkS) is the pioneer work on an intrusion fault tolerant approach for WSN (Challal et al., 2011). The basic design of INSENS deals with the challenge of fault tolerant and security issues (Deng et al., 2006). In addition to multipath routing, INSENS achieves the design goals via the integration of lightweight security mechanism such as one way hash chains and nested keyed message authentication codes. The protocol INSENS reduces the complexity presented by resource-poor sensor nodes towards the maximum utilization of resource-rich base stations. The computation, communication, storage, and bandwidth requirements at the nodes are reduced, but at the cost of greater computation and communication at the BS. Control information pertaining to routing is authenticated by the base station using the one-way hash function to prevent masquerading by a malicious node and injection of false routing data. INSENS constructs routing tables in each node and only the BS is allowed to deploy and disseminate routing tables throughout the network. INSENS builds multiple independent routes to bypass compromised nodes and to route messages correctly in the presence of adversaries and failed nodes. Thus, the forwarded packets can still reach the destination without passing through the malicious node.

The INSENS protocol consists of two parts: route discovery and data forwarding. Figure 5 shows the INSENS routing phases. Route discovery develops the topology of the sensor network and sets up the forwarding tables at each node by exchanging control messages. It is performed in three phases: (i) the base station securely floods a request message to all sensor nodes in the network, (ii)
sensor nodes securely send local topology information via a feedback message back to the base station, and (iii) topology information verification at the BS, computes the multipath forwarding tables for each sensor node, and securely unicasts those tables on a breadth-first basis to the respective nodes using a routing update message. They use the tree-structure methodology in multi-hop multipath data forwarding. The data forwarding phase takes place based on the forwarding tables computed by the BS. In order to respond against attack, INSENS blocks all its downstream nodes by simply dropping feedback messages. Moreover, keyed MAC plays an essential role to authenticate each node, the paths to the base station from each node, and neighbor information of each node. Such benefits of INSENS rely on its ability to tolerate disruption caused by an intruder who has compromised deployed sensor nodes, and against malicious attacks. INSENS incorporates efficient one-way hash chains as one-way sequence numbers to limit the ability of an adversary to flood the network. Nested keyed message authentication codes are used to uniquely and securely associate a MAC with a node, a particular path, and a specific One-way Hash Chain (OHC) number to defend against replay attacks through wormholes in the routing set up phase and the data forwarding phase. However, INSENS has limitations in terms of security, scalability, and maintenance issues. In addition, INSENS inhibits malicious attacks by using the assumptions that a secret pairwise key is shared only between the BS and a sensor node. Since the routing tables of sensor nodes are computed in sink nodes, the computation cost to distribute the routing tables is increased, especially in large-scale sensor networks. Moreover, the use of a global key for secure neighbor detection affects the whole network performance once the global key is compromised (Kumar and Jena, 2010).

6.4.3. Enhanced INSENS

In order to address the limitations presented in basic INSENS, an enhanced version of INSENS is introduced by consolidating: (a) bidirectional verification, (b) the multipath mechanism, and (c) a pair-wise key setup scheme in the routing protocol (Fig. 6). The bidirectional verification is employed to defend against rushing attacks. The multipath scheme is proposed since the enhanced version can scales to larger sensor networks; moreover, the multiple base stations in the network are able to construct multiple paths efficiently. As a consequence, it can significantly minimize the number of nodes that can be blocked by an adversary who manages to compromise the sensor node. Also, the pairwise key setup scheme is imperative for the secure maintenance mechanism to manage the activity of node joining and leaving throughout the network. This circumstance is presented overhead of cryptographic algorithms. However, the enhanced version of INSENS works well against wormhole attacks. Furthermore, with multiple base stations, a base station doesn’t need to compute the routing paths for sensor nodes, nor contend with large-sized feedback messages or routing tables. This significantly improves the scalability of INSENS and as a
result, the enhanced INSENS can be used for secure routing in large sensor networks. In the enhanced INSENS protocol, a sensor node needs to save a global key, pairwise keys, cluster keys, one-way hash chain numbers, and several random numbers for new node authentication. Also, the maintenance of multiple paths to the multiple base stations from each node causes
excessive overhead for each sensor node, since every node is potentially a source node in sensor networks.

6.4.4. MVMP

The design of the Multi-Version Multi-Path (MVMP) routing protocol is built with a major concern for fault tolerance so that the overall sensor network functionality can be sustained even in the presence of node failures (Ma et al., 2007). In the network model, MVMP is deployed based upon four important assumptions: (i) multiple paths have been set up in the network before the data transmission, (ii) the BS is resource-rich and cannot be compromised, (iii) the base station and individual sensor nodes have pre-built cryptographic algorithms and pre-distributed keys to generate the session keys before the deployment of WSN, and (iv) the selected cryptographic algorithms and keys are able to meet the resource constraints of the current generation sensor nodes. In order to achieve both secure and reliable data transmission, the proposed protocol integrates: (a) data segmentation, (b) forward error correction (FEC) coding, (c) multipath, and (d) multiple versions of cryptographic algorithms. FEC coding operates by adding redundancy to the transmitted information using a predetermined algorithm. The advantage of FEC is that data retransmission can often be avoided. Therefore, the FEC mechanism is used in situations where retransmissions are relatively costly or impossible. The Reed Solomon (RS) code is selected to achieve reliable data transmission in networks. As shown in Fig. 7, there are three phases involved in the data transmission of the MVMP mechanism: (a) sending, (b) data delivery, and (c) receiving process. With MVMP, different parts of the data will be encrypted using different cryptographic algorithms before being sent to the destination via different paths. MVMP adopts MD5 with hash message authentication code, Skipjack, and CCM modes for authentication and integrity check. MVMP allows secure data transmission since the adversary should be aware of all the encryption algorithms supported by this protocol.

MVMP mechanism reduces the chance of an intruder being able to intercept and decrypt all parts of the data since the adversary must compromise all the code words transmitted along multiple paths to capture the original message. Therefore, MVMP is successful for achieving simultaneous fault tolerant and intrusion tolerant data transmission in WSN. The drawbacks of MVMP rely on the network model assumptions where the BS and each sensor node has pre-built cryptographic algorithms and pre-distributed keys to generate the session keys before the real deployment of WSN. Furthermore, MVMP claims its protocol is highly secure because of the multiple encryption algorithms implemented for different parts of the data information, which are transmitted along the multiple paths. It uses the multi version of the cryptographic algorithm including secret-key cryptography (SKC) and public-key cryptography (PKC) to provide authentication and integrity in data communication. However, they are not considered the details of multiple routes discovery, cryptographic algorithms implementation, key distribution, and management in MVMP routing. As it uses different cryptographic algorithms, the cost of resource constraints is increased.

6.4.5. SEIF

The SEIF (Secure and Efficient Intrusion-Fault tolerant) routing protocol presents an intrusion-fault tolerant routing scheme by offering a high level of reliability via a secure multipath routing (Ouadjaout et al., 2008). This protocol relies on a distributed and inter-network verification scheme, which does not require any reference to the BS. A new multipath selection scheme is employed to enhance the tolerance of the network and minimize the energy consumption. Also, SEIF provides authentication requirements through an efficient symmetric cryptography mechanism called one way hash chain. Particularly, round sequence numbers, sub-branch tags, and parent requests are authenticated using the one way hash chains. SEIF consists of three phases: (a) bootstrapping, (b) tag distribution, and (c) tree construction. The main purpose of the bootstrapping phase is to initialize the

![Fig. 7. The main phases in MVMP routing.](image-url)
different types of chain verifiers. The tag distribution phase is important to provide each sub-root with its valid tag. The final phase is constructed as sub-roots that initiate the construction of their sub-trees. Figure 8 illustrates the routing process in SEIF.

The sink uses an OHC to generate round sequence numbers and each round is identified with a sequence number that is the last delivered value of the OHC. Hence, the authentication requirement of round initialization is satisfied. Therefore, the intruder cannot initialize the construction of a new tree on behalf of the sink. Furthermore, SEIF provides authentication of sub-branch tags to prevent an intruder from forging valid tags on behalf of the sink. When the sink starts a new round, it distributes to the sub-roots their respective tags, which represents the next unrevealed value of distinct OHC. Also, SEIF provides authentication of route construction requests relayed by the parent nodes to circumvent an intruder forging the route requests on behalf of legitimate nodes. To ensure parent authentication, each sensor uses a local OHC providing sequence numbers for its local broadcasts by one hop broadcasts. With the in-network verification scheme, sensors rely only on local information to successfully detect forged routing messages. Therefore, any intrusion attempt is promptly detected without additional delay. To evaluate the capability of secure multipath protocols to tolerate the presence of intruders and failures, the resiliency of SEIF is evaluated against different routing schemes with respect to the ratio of the minimum number of compromised and failed nodes that can disconnect the constructed topology making sensors unable to reach the sink node. The OHC mechanism ensures the authentication of exchanged control messages without incurring high energy consumption. However, the process of authenticating each sub-root with a valid tag increases the delay in the whole network communication.

6.5. The prevention-based approach

WSNs by nature are unattended and vulnerable to physical attacks in the form of node capture or node destruction. Thus, secure multipath routing with a prevention-based approach is important to thwart an intruder from inserting compromised nodes. In order to achieve the goal, the protocol needs to consider the limited capabilities of sensor nodes. Also, the corresponding secure routing protocols require additional support from variant kinds of security infrastructure which is necessary to provide protection throughout the WSN attacks aimed at endangering the network performance. This section reviews existing solutions for secure multipath routing with a prevention-based approach.

6.5.1. SEEM

The Secure and Energy-Efficient Multipath (SEEM) routing protocol focuses on extending the network lifetime and providing security in WSN (Nasser and Chen, 2007b). Each of the nodes in SEEM needs to keep the information of the routes in the routing tables, which refer to potential neighbors that are able to forward packets to the base station. The uniqueness in SEEM relies on its capability to select a routing path using BS instead of depending on the source or sink node. Hence, it defends specifically against
attacks on routing protocols that attract traffic by advertising a high quality route to the BS. The concept used by SEEM is similar to the client/server architecture where the BS takes the role of the server and sensor nodes act as clients. The base station is responsible for route discovery, route maintenance, and route selection. It then selects a new path from the available paths based upon the current energy level of nodes along each path. The multipath technique used in SEEM improves the energy consumption in data routing. In the shortest path selection phase, SEEM modifies the Breadth First Search (BFS) algorithm to consider the energy, (i.e., the weight corresponding to each edge) of each node. If one node on the shortest path has less energy left than required level, then this shortest path is discarded and continues searching for the next shortest path. SEEM takes into account many assumptions on energy; such that the energy consumption for each task is known for specific application, thus it neglects the energy for computation. Also, it is assumed that each node consumes the same level of energy for transmitting and receiving one packet. Figure 9 shows the basic phases in SEEM: (a) topology construction, (b) data transmission, and (c) route maintenance. In the topology construction phase, the network topology is deployed, whilst the data transmission phase involve the important operational phase, (i.e., the sensor network starts its task), and in the route maintenance phase, the BS updates the amounts of available energy on each node, participating in the communication, and re-selects a new path to the source node.

Based upon the character of advertising an attractive route to the destination, SEEM is resistant to specific attacks such as wormhole, sinkhole, and selective forwarding. SEEM is designed based on multipath without the need for other security mechanism support. However, the assumptions made for the energy conditions are ineffective for an energy-efficient routing protocol. In addition, the SEEM protocol justifies the security without any encryption and authentication mechanism. Moreover, the simple link layer encryption and authentication using a globally shared key is not considered for security purposes since the routing path is solely selected by the BS. Hence, the data packets can be modified in transmit. Furthermore, SEEM leaves a lot of burdens on the BS since it has to deal with the decision-making process, including querying specific sensing data, broadcasting control packets, routing path selection, and route maintenance. Also, SEEM considers that the sink node needs to update the information of the whole network topology which consumes excessive energy and introduces extra overhead.

### 6.5.2. HSNRP

The protocol proposed by (Abid et al., 2009) is developed on heterogeneous sensor networks, which operate in clusters to reduce energy consumption. This multipath routing protocol aims to bypass intruders and decrease the routing overhead. The cluster formation data is processed locally where the base station generates inter-cluster routes and the cluster head generates intra-cluster routes to reduce communication and computation loads on centralized BS. In the heterogeneous sensor networks routing protocol (HSNRP), routing tables are generated with multipath routing. This provides a lightweight broadcast authentication to secure routing table generation and data communication. A small number of high power nodes work as cluster heads (CH) and large number of low power nodes work as cluster nodes (CN). It is assumed that BS shares unique secret keys with each CH and CH are pre-loaded with keys that they shares with their CNs. The
implementation of security architecture within routing protocol design consists of two main parts: a) route discovery and b) data forwarding. Figure 10 illustrates the routing mechanism in HSNRP. It is assumed that CNs use shared pair wise keys for authentication of messages transferred between CH and CNs. The CNs are pre-loaded with Bloom Filters (BFs) and hashed TESLA instances, which are required for one way broadcast authentication. The route discovery phase consists of three sub phases: (a) route request message is broadcasted from the BS to all of the CHs and CHs re-broadcast to their entire CNs, (b) all CNs send their topology information to CH via route response message, and (c) CH computes forwarding tables for each CN based on the information received. CHs generate pair-wise keys for each pair of neighbor nodes that are on same path. Then CHs send routing tables and pairwise keys to each CN and aggregated data to the BS. The details of each sub phases is described as follows:

(a) BS commences to create the network topology as it needs to construct routing tables. CH discovers multiple routes to any destination. HSNRP uses the hybrid technique of TESLA and Compressed Bloom Filters to check if the ROUTE REQUEST message is initiated by the BS at CH level and from CH at CN level. It is assumed that all CH and CN have one BF preloaded with keyed hashed values for authentication purpose. HSNRP consider a set U of independent TESLA instances containing N number of keys (k) where the last N keys of TESLA are hashed and entered to m-bits BF. On receiving ROUTE REQUEST the message receiver checks for the instance (k_{c+1},...,k_{c}) used to generate the Message Authentication Code Request (MACR) using a one-way hash function. It then queries BF for the presence of the hash of the instance. The whole network time is divided into epochs and the message counter at the sender node is reset. The number of broadcast messages by each node per epoch is bounded to k. If the adversary replays the old legitimate ROUTE REQUEST message, it is prevented from using BF. Each node has two BF for two epochs i.e. E_{c} current epoch and E_{c-1} the previous. All of the valid messages received in epoch E_{c} are stored in BF_{c} using the one-way hash function on the counter value and source identity and BF_{c-1} has all the legitimate messages of the previous epoch E_{c-1}. To prevent the malicious node using a fake path, each message is appended with MACR calculated using K_{CH_{c}}, CN_{j} before forwarding to next node. The 16-byte MACR is calculated by node, say, A, over the complete message, including node A own appended identity. Only the last 64-bits are appended to the message to minimize the overhead, where, this overhead is for the period of route discovery and the routing table formation phase. MAC is generated using the secret key of node ‘A’ using the following values:

\[ MACR_{A} = MACR(AM; Len; path; key_{A}) \]

where AM defines an active message type to help sensor nodes know that CH is collecting topology information for the routing table construction, ‘Len’ contains the length of the path, the path field contains the path from CH to the current CN. MAC is for the integrity of the paths.

(b) In the second phase, ROUTE RESPONSE is returned to the initiator of route discovery. Each node ROUTE RESPONSE message consists of a path-sequence from an upstream neighbor that broadcast this ROUTE REQUEST message to the node, chosen-parent, and its local connective neighbors. For the
secrecy of REQUEST RESPONSE returned to CH, 16 bytes of Message Authentication Code Response (MACRR) is calculated and appended to message. The third phase is performed in routing tables generation and propagation to each node where the CH, after broadcasting the ROUTE REQUEST message waits for a certain period, during which it receives local connectivity information from all CNs, through their ROUTE RESPONSE messages. Security mechanisms during the previous phases guarantee that information that reaches BS via CH is secure. Further, CH computes MACRR for each ROUTE RESPONSE message, and compares that with the received message. If the two match it goes further for neighbor’s connectivity information. BS generates a multipath between the same sender and receiver using the shortest path algorithm and sends ROUTING TABLE with neighbor information of the CHs. The CHs then generate the routing table and pair-wise keys for cluster members and send that to each node. The ROUTING TABLE of each node is encrypted using key $K_{CH_i, CN_j}$.

In the data forwarding phase, nodes can communicate through their neighbor nodes on routes directly using pair-wise keys generated by CHs to encrypt the message sent to destination nodes. The message includes sender ID, receiver ID, and destination ID. On receiving message node check for the destination ID, if it is present in neighbor list, it forwards the message to the next node. The multipath is discovered and the message is forwarded on the available paths to prevent the message from undergoing selective forwarding or sinkhole attacks. Message integrity is assured by encrypting it; authentication and replay protection is guaranteed using TESLA and BF.

The security analysis of HSNRP is in comparison with the protocol INSENS. The analysis of the HSNRP shows that it is secure against routing attacks and tolerant to compromised nodes. The node receiving the ROUTE REQUEST needs to check the validity of the message by computing its keyed MAC. The receiver has to ensure that the message is not replayed. The BF stores messages of current and previous checks to secure nodes from replay attacks. If the node is compromised, its cryptographic data is also captured, but CNs only have a limited number of keys that they share with their neighbors and one secret key that they share with CH. Since each node shares a unique secret key with its CH and pair wise key among its neighbor nodes, the adversary cannot perform multiple identities to launch a Sybil attack. However, HSNRP considers many assumptions on pre-loaded keys.

6.5.3. STAPLE

The STAPLE (Secure routing and Aggregation Protocol with Low Energy cost) routing scheme integrates a multipath mechanism and one-way hash chain to achieve security in sensor network (Gui et al., 2009). The network expanding model is proposed to control...
the communication cost incurred by multipath and to minimize energy consumption. The proposed protocol involves three important phases: (a) initialization, (b) data transmission, and (c) source authentication. Figure 11 depicts the phases involved in STAPLE. In the initialization phase, the sink node generates a random number to produce keys to authenticate code for source nodes. The process continues with finding neighbors in one hop, and then expands hop by hop to the edge of the sensor network. Since sensor nodes contain the information of neighbors and know the direction of the sink node, they could find their parents or children and construct routing paths from source nodes to the base station. The parents utilize hash-based message authenticated code (HMAC) functions to generate keys for children, hence generating the one-way hash chain. Furthermore, multiple parents can build multipath routing to tolerate node failure. After the initialization phase, the parent nodes receive packets from their children. Therefore, the parents re-generate children’s keys and authenticate their identity to filter out false data packets. In the subsequent phase, HMAC is adapted to achieve authentication and data integrity. It also uses symmetric cryptography to provide data secrecy. The sink node re-generates source node’s key with a random number to authenticate the source node’s identity and data integrity to prevent intermediate nodes from forging data packets, because only the sink node keeps the random number.

However, STAPLE has a drawback since they did not consider the maintenance of the multipath and key production. The performance of STAPLE is compared with INSENS, and the founders of STAPLE claim that their protocol has a better performance in comparison with INSENS and achieves a higher level of security. In addition, the results show that STAPLE makes better use of network redundancy, and it can tolerate larger node failure ratios of sensor networks. In large-scale sensor networks, the performance of STAPLE is similar with that of INSENS.

6.5.4. EENDMRP

The Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) is proposed to find multiple paths based on the rate of energy consumption and filled queue length of the node (Gaurav et al., 2012). The digital signature crypto system is applied to enhance the security performance by adopting the MD5 hash function to generate the digital signature whilst the RSA algorithm is used to produce a pair of private and public keys. To prevent the formation of paths with loops, the network is assumed to consist of a number of stages based upon the number of hops between the source and destination. The sink node constructs multipath routing to generate the routing tables.

EENDMRP consists of two phases namely, (a) route construction and (b) data transmission. The sink node initiates the multipath route construction to generate its routing tables as illustrated in Fig. 12. Route CONstruction (RCON) packets are exchanged between the nodes, then each sensor node broadcasts the RCON packet once. The neighboring nodes receive the RCON packet updates RCON packet with its public key. It rebroadcasts the RCON packet to its neighboring nodes. Correspondingly all the nodes in the particular network update their routing table with their neighboring node’s public key. In the data transmission phase, the source node selects the node-disjoint paths to the sink node and sends the data traffic via multipath. The primary path is chosen from the available node disjoint multiple paths between source and destination based on maximum Path Cost (PC) based upon effective node parameters like, rate of energy consumption, filled queue length, and effective residual energy. The security in EENDMRP is designed using the public key crypto system. MD5 hash function is used to generate the digital signature, whilst the private and public keys are generated using the RSA algorithm. It is assumed that all the sensor nodes have their unique public key upon its deployment. The neighboring nodes update the route construction packet with their public key and rebroadcast to the intermediate nodes. Also, every node should know the public key of its neighboring node (i.e., reachable in one hop) to update their routing table. The MD5 hash function creates message digest at the source node, then the source node generates a digital signature by encrypting the message digest with its private key and forwards the authenticated data to its neighboring node through the selected path. If the verification value (i.e., generated message digest by the receiver and the decrypted message digest of digital signature) is equivalent, then the receiver accepts the data. In case of the data being altered upon transmission, the route error packet is created to notify the sender. The primary path is chosen from the node routing table based on the maximum path cost using the short filled queue length of the node. If any node’s filled queue length is maximum in a path, the chances to be selected as a primary path is reduced. The effective primary path selection mechanism in the EENDMRP avoids packet dropping after the queue is filled. Also, EENDMRP ensures the correctness of data, non-repudiation, and authentication. Since a new metric measuring energy with link reliability is yet to be designed, the energy performance of EENDMRP raises concern about the practicability to ensure better energy and security performance simultaneously.

6.5.5. mEENDMRP

The mEENDMRP (Modified Energy Efficient Node Disjoint Multipath Routing Protocol) proposes a modified version of the EENDMRP by considering transmission range adjustment to improve energy efficiency (Sangeetha and Yuvaraju, 2012). Before the transmission range can be adjusted based on their neighbor node’s location, node disjoint multiple paths are selected for data transmission to spread the load among different nodes. The main idea of transmission range adjustment is to minimize the energy consumption of WSNs. Therefore, if the neighbor node is nearer, the transmission range will be reduced. Also, a high transmission range of a node can be adjusted to a low transmission range, which is important to increase the network lifetime. For security provisioning, a digital signature based cryptographic system is used with the RSA algorithm and MD5 hash function. mEENDMRP consists of two phases, routing table construction and data transmission as shown in Fig. 13. In order to construct the routing table, distance exchange and public key exchanges will be performed. If the route construction packet is received by any node, then its route construction sequence number will be incremented by 1 before forwarding. In the data transmission phase, through the maintenance of multiple paths, the data is transmitted on the primary path.

The decision on selected primary path is computed based on the path cost and primary path selection. Path cost reflects the cost of the node in terms of minimal residual energy in the path. Hence, the path with the maximum path cost is chosen as the main path in primary path selection. Based on the selected primary path, all the other paths will also be constructed. The number of multiple paths will differ based on the size of the data load. If the data load is minimal then the number of paths will be less and vice versa. After selecting the multiple paths, the transmission range of the nodes present in the multiple paths will be adjusted as per the distance between them using selected techniques and algorithms. In addition to the consideration of the exact transmission range, mEENDMRP selects different levels for the transmission range.

The document will be digitally signed by the sender before beginning the transmission. The receiver will check the digital signature to ensure the authenticity of the document. The MD5 hash function is responsible for producing the message digest. If the
decrypted digital signature is equal to the message digest, the message is considered valid. In the security domain, prevention of different types of attacks is satisfied through using the multipath and asymmetric key crypto system. This protocol provides network reliability by avoiding holes through load balancing and effective multipath selection based on the primary path. Besides the complexity of cryptographic, calculating the exact transmission range may lead to intricate calculations and high energy consumption on a node.

6.6. Mixed-mode approach

Given the rapid development of WSNs in various applications, the tolerant, detection, and prevention-based support have become essential to achieve the security requirements and provide countermeasure against WSN attacks. The mixed-mode approach is required since some forms of attacks are difficult to protect against. In addition, multipath routing requires support from some security infrastructure in order to alleviate the chances of potential attacks interception in WSN. For instance, detection against attacks is one of the important challenges in sensor network security (Chen et al., 2007). The detection schemes are targeted to identify the success of packet delivery in data routing, to pinpoint the misbehavior of their neighbor node based upon the observation of behavior of the nodes, and to reduce the effect of malicious nodes via locating the compromised nodes at the initial stage of routing. With the mixed-mode approaches, it is imperative to build security within the network architecture and protocols, and therefore a WSN can successfully operate in the presence of component failures or malicious attacks or both. This section discusses some of the research in this area.

6.6.1. SeRINS

In SeRINS (SEcure alternate path Routing IN Sensor networks), the sensor nodes set up a routing tree with a base station as the root (Lee and Choi, 2006). The BS can directly transmit data to any node in the network, whilst a sensor node sends data along the multi-hop route to the base station. SeRINS assumes that the BS shares a unique secret key with every node in the network and each pair of neighboring nodes establishes a secure communication channel by agreeing on a unique secret key between two neighboring nodes. The multipath is used as an alternative mechanism to defend against selective forwarding attacks. As
shown in Fig. 14, this protocol implemented three basic schemes in its design: (a) an alternate path scheme, (b) neighbor report system, and (c) neighbor authentication. An alternate path scheme is developed to establish a new routing topology. The neighbor report system is imperative to make the network resilient to several compromised nodes. It can detect and exclude the compromised nodes, which inject inconsistent route updates, from the network by using hop count verification based on reports from neighbor nodes and perform node revocation by the BS. Neighbor authentication is important to control routing advertisement which is a locally broadcast message. In order to avoid delay in authentication of routing advertisements, an efficient mechanism for broadcast authentication is required. The ARMS mechanism is employed to provide immediate authentication, with a small memory space and no clock synchronization. It helps prevent a routing message from being spoofed and altered. Using a neighbor report system, a base station gets to know which node is compromised and excluded from the network, and then it broadcasts the information about the compromised node (e.g., node ID) to the whole network. By network-wide revocation of the cryptographic keys of the compromised node, SeRINS is able to exclude the compromised node from the network. Therefore, it is resilient in the presence of spoofed, altered or replayed routing information, selective forwarding, sinkhole, and HELLO flood attacks. However, SeRINS can perform only partial verifications that limit the ability of sensors to make local decisions in the presence of compromised nodes. Indeed, when a sensor detects a suspicious packet, it alarms the sink which needs to gather data on the suspect node from its neighbors. Since the process is achieved via successive broadcasts, the cost is expensive in large networks causing additional delay and overheads to detect the intruder.

6.6.2. PRSA

The path redundancy based security algorithm (PRSA) (Al-Wakeel and Al-Swailem, 2007) uses alternative routing paths for each data transmission to overcome sensor network attacks. The idea behind the PRSA algorithm is to find secure multiple and lowest cost routing paths between the source and destination nodes by removing the node that is suspected as an active adversary node from the routing
A node can be identified using a set of parameters that usually reflect the presence of adversary nodes (e.g., low link cost in sinkhole attack). Other parameters include node power, number of hops to destination, node HELLO messages, and a combination of node ID number and power. The paths can be either disjoint or braided. Disjoint paths differ in all path links and nodes, while braided paths have only one or more different nodes among the selected paths. To enhance the routing security and network reliability, PRSA allows source node data packets to be sent on the identified routing paths using three types of transmission modes: (a) redundant, (b) round robin, and (c) selective modes. In redundant mode, the packets are re-transmitted on all paths simultaneously, while in round robin, each packet is sent on an alternate path one at a time in a round robin fashion. Meanwhile, the selective mode selects the highest cost shortest path to send all call packets through. The link cost is evaluated based on a combination of distance, energy, and bandwidth measures, depending on the network topology and design. Symmetric routing for connected nodes is assumed to find the optimum shortest path between source and destination (using the Dijkstra algorithm). The PRSA algorithm is applied to find alternative paths by removing all or some of the primary path nodes according to paths whether paths are disjoint or braided. It also selects the transmission mode for the call packets (redundant on all paths, round robin, or selective over a given path) and simulates the packets transmission. The performance results prove that the algorithm improves sensor network resistance and reduces network vulnerability to security threats. The PRSA mechanism is also evaluated against the different transmission modes and shows better network performances in terms of delay and network overhead even in the presence of compromised nodes. Although the PRSA is effective in terms of reliability, it is not been evaluated against existing secure multipath routing and various routing attacks in specific way. Figure 15 shows the routing process involved in PRSA.

6.6.3. SELDA

The SEcure and reliable Data Aggregation (SELDA) routing protocol proposed a secure and reliable data aggregation protocol using the establishment of a web of trust (Ozdemir, 2007). Beta Distribution function was adopted to compute the reputation value of a sensor node. The sensor nodes transmit their data to data aggregator(s) over one or more secure paths based upon the trust levels. During the data aggregation phase, the aggregators weight the data based on the trust levels of the sender nodes. Sensor nodes and data aggregators monitor their environments periodically to detect the misbehaviors of their surrounding nodes and quantify those observations as reputation values of those nodes. Reputation values are then exchanged among sensor nodes in order to determine reliable data aggregators and secure paths to those data aggregators. An attacker node may degrade the network’s performance by not cooperating with other sensor nodes. Therefore, if a sensor node does not respond to hello messages over a period of time, the reputation value of the node availability is reduced. Moreover, if a sensor node does not respond to hello messages in its active phase; it can be detected by one of its neighbors. In addition, a compromised node may not forward the received data packets to the destination node or misroute them by changing the destination address. Routing misbehaviors can be detected by neighboring nodes using watchdog mechanisms.

The basic idea behind the protocol SELDA is that compromised sensor nodes are likely to have lower reputation values as compared to the normal sensor nodes. Figure 16 shows the data aggregation scenario in SELDA. At the data aggregation process, the data security of each sensor node is verified based upon its reputation value to reduce the effect of compromised sensor nodes on the aggregated data. This is achieved by employing a reliable data aggregation algorithm on each data aggregator which is imperative to minimize the effect of false data sent by the data
aggregator’s compromised neighboring nodes. In addition, a secure multipath data transmission algorithm is proposed to mitigate the effect of message forgery that may disrupt the network traffic by selectively forwarding or misdirecting packets and to ensure secure data delivery to data aggregators. The proposed algorithm allows the sensor nodes to send their data using a special packet header. Therefore, the algorithm secretly selects some paths based on the reliability of the paths and keeps the quantity and identity of the selected paths secret. The performance evaluation of SELDA shows that it improves security and reliability in terms of communication overheads as well as the efficiency of multipath data transmission even in the presence of compromised nodes. A data aggregator computes a reputation value for each neighboring sensor node whilst a sensor node computes a single reputation value for its neighborhood to reduce the computational overhead. Since the sensor nodes and data aggregators differ in computing reputation values, there is an excessive cost in terms of computation. In addition, the computation result can be redundant.

6.6.4. SCMRP

The SCMRP (Secure Cluster based Multipath Routing Protocol) proposes clustered sensor networks and multipath sensor networks, which aimed to increase the network efficiency and to increase the resilience and reliability of the network respectively (Kumar and Jena, 2010). In order to provide sufficient security to the sensor network, SCMRP adopts the proper use of cryptographic algorithms. Also, SCMRP is designed to deal with security, orphan nodes, and multi-hop issues in clustering protocols. At initial deployment, each sensor node has a unique identification (ID), a certificate (CERT) that is signed by the base station, a unique shared key (shared with BS), and a public key of the BS. The certificate is used to authenticate any node at the time of neighbor detection with the public key of the base station, whilst the unique shared key is used to communicate with the base station. In order to detect neighbor behaviors, the node starts broadcasting and receiving the neighbor detection packet, which contains the ID and CERT of the node. Each node that receives the packet will authenticate the node ID by verifying the certificate. If the sender node is authenticated, the receiver node will then attach its ID to the neighbor list, otherwise the packet is discarded. Hence, the unauthorized node is prevented from interfering in the neighbor detection phase. BS calculates the secret key (i.e., pairwise key) for every pair of neighbor nodes and constructs the network topology based upon the collected neighbor information of the network. Also, BS produces a neighbor matrix to find the multiple paths. After the end of this phase every node pair possesses a pair-wise key. Hence, the formation of the cluster is initiated by the BS. Election of the cluster head is based on the residual energy.

The data transmission phase consists of three components: (a) the member node transmits the sensed data to the cluster head in the encrypted and authenticated form, (b) the cluster head aggregates the received data to the new signal and sends it to the BS with the appropriate route, and (c) the BS will use the unique shared key (with CH) to decrypt and authenticate received data. As the data reaches the BS through the prescribed route, the BS uses the unique shared key to perform data validity. In the re-clustering and re-routing phase, the BS continuously monitors the residual energy of the existing CH, if found below the threshold value it elects another CH. After electing the CH, the network repeats a similar procedure to form a cluster. SCMRP deals with the issues of the key management, new node, and orphan node.
When dealing with the key management issues, each node has to associate with a unique shared key with the base station, ID, certificate, and a public key to prevent eavesdropping or altering of message by adversaries. Therefore, any node that needs to send a message to the BS needs to perform encryption and create a MAC with the unique shared key, so only the BS can access it. The orphan node generally has neighbors but is not associated with the CH. SCMRP restricts the number of orphan node requests by allowing them to send a route request to the BS. After getting the route requests, the BS sends a route reply by computing the routing path. Thus, the routing path reaches the orphan node and it can send the sensed data to the BS, till it does not get any clustering request from the CHs. Figure 17 depicts the routing process in SCMRP.

This approach is beneficial in the application where each and every sensor node’s data is precious since the increment of the orphan node decreases the performance of the network. In the SCMRP, the routing paths are computed and maintained by the BS. Therefore, whatever an adversary performs, it has no impact on the selection process of the routing path. SCMRP provides security against various attacks such as selective forwarding, sinkhole, wormhole, and Sybil attacks. However, the routed packets,
neighbor information list, and pair-wise key received by the BS consumes high energy and memory in the resource-constrained WSNs.

6.6.5. MSR

The MSR (Multipath Secure and Reliable routing protocol) is considered a homogeneous network, where all uncompromised
nodes have the equivalent hardware and software capabilities (Moustafa et al., 2011). There are three important components derived by MSR (Fig. 18): (a) on-demand routing, (b) enhanced Passive Acknowledgment (PACK), and (c) erasure coding. The process of discovering multiple paths routing is performed in a reactive manner to reduce the routing overhead. In addition, on-demand multipath routing provides an easy mechanism to distribute traffic and balance the network’s load. In order to form multipath routing, MSR consists of two essential phases namely route request and route reply. The PACK refers to the sender passively listening to the channel after finishing the packet transmission to confirm that the packet has been received by the destination. This comes indirectly by overhearing the next node forwards the packet to its next hop neighbor. If a node does not get a PACK, it times out and retransmits the packet. In MSR, the benefit of PACK is enhanced by leveraging it to detect security attacks by analyzing the overhead packets. The erasure coding component improves reliability in WSNs with less overhead. Moreover, it can convert a message into a set of coded shares so that any sufficiently large subset of the coded shares can be used to reconstruct the original message. MSR adopted erasure coding to enhance the reliability and security of its operation in WSNs. Also, it can be used to divide an original message into sub-packets and send these sub-packets via multiple paths. The destination has to compile these sub-packets to construct the original message.

The integration of multiple paths and erasure coding in MSR reduces the probability for an attacker to completely stop the packet flow in data transmission. Hence, MSR enhances the security of WSNs under different attacker models. It concludes three different categories of attacks: (i) attacks that can be completely prevented (spoof, alter, and replay routing information, selective forwarding and HELLO attacks), (ii) attacks whose effect is reduced (sinkhole and wormhole attacks), and (iii) those that still need to be addressed by other mechanisms (i.e., Sybil attack). The limitations of MSR rely on the use of PACK since it refers to the sender passively listening to the channel after finishing the packet transmission to ensure that the packet has been received by the destination. In between the process, the secrecy of data can be accessed and manipulated by the compromised node.

6.6.6. SeMuRa

SeMuRa (Secure Multipath Routing Algorithm) proposed a secure on demand routing algorithm that should be tolerant to attacks (Triki et al., 2012). In SeMuRa, the concept of $k$-connectivity is extended to $k$-$x$-connectivity where $x$ is the disjointness threshold that represents the maximal number of nodes shared between any two paths in the set of $k$ established paths. Labels in the datagrams are used to exchange in the route discovery phase to attach the threshold $x$. Besides multipath, SeMuRa relies on the advantages of an elliptic threshold signature and watchdog mechanism to tolerate routing attacks. Also, the proposed algorithm must be distributed where intermediate nodes should start learning and gathering information regarding potential available path as soon as the route request datagrams propagate. Most of the multipath routing algorithms establish maximal disjoint paths, thus node performance is severely affected and resources are exhausted, especially if the routes include many hops and the nodes density is high. To overcome this limitation, SeMuRa extends the multipath routing algorithms so that a disjointness threshold will be defined and exploited during the route discovery to create a trade-off between fault tolerance and network performance. Before sending data, a sensor node should ensure that a set of $k$ paths are available between itself and the base station. Then it sends duplicated copies of data over the alternative paths to decrease the probability of communication failure. SeMuRa consists of two steps: route discovery and route maintenance, which allow discovering and maintaining possible multiple paths between any sensor source node and the BS as shown in Fig. 19. The route discovery phase is initiated when the source node wants to establish a set of paths with the BS. The on-demand properties allow SeMuRa to minimize the overhead and specify the path-disjointness threshold value. After receiving a list of potential paths, the sensor source node computes all paths to the destination that satisfy the specified threshold, lists the potential paths, caches the remaining ones, and starts sending the data. Thus, keeping information regarding unused paths allows a rapid reaction to routes modification and decreases the overhead related to the generation of a new route request packet. In the route maintenance phase, the sensor source node updates the list of paths in use if the network topology changes or some routes are broken due to an attack or sleeping cycles of nodes. This mechanism is based on letting intermediate nodes use the watchdog concept for every packet they forward in order to detect the identities of misbehaving nodes or routes errors. If the next hop appears to be broken, a route error packet is generated and sent to sensor source node to decrease the number of possible paths to the destination. A combined method is proposed which is based on the integration of a watchdog mechanism and digital signature to enhance security in SeMuRa. The watchdog mechanism is used to let a node detect whether its neighbor is forwarding the datagram received from another node and to capture several types of routing attacks (e.g., wormhole attacks). The values of the two parameters $x$ and $k$ are highly correlated and both of them depend on the node density. Typically, if the source node chooses a high value of $k$, it should tend to decrease the value of $x$ to guarantee the establishment of all paths. False positives may occur if a node detects that its neighbor is malicious because it has not forwarded the datagram and if the state of a node involved in the route to the BS sleeps or runs out of energy. Such nodes, which are not detected as inactive yet, may be considered as malicious and lead to the generation of false negative alerts. For security purposes, the proposed algorithm should verify that packets are correctly forwarded in the networks and identities of intermediate nodes are appended securely based upon the routing requests. Moreover, the algorithm should generate evidence of identities and node behavior that takes part in the establishment of the multiple routes. This is important if a digital investigation scheme is used to trace back an attack that occurred, locate the malicious nodes, and ascertain the presence of forged routes. Nevertheless, SeMuRa relies on an asymmetric digital signature for the authentication, which results to very high overhead to create and verify the signature. Further, the identification of captured nodes based on the applied watchdog mechanism and intermediate signature increases the consumption of network resources which is not cost effective.

6.6.7. BEARP

BEARP (Based on Encryption and Authentication Routing Protocol) efficiently combines the security and energy efficiency issue in its proposed framework (Zhou, 2013). It consists of three phases: neighbor discovery, routing discovery, and route maintenance. BEARP encrypts all communication packets and authenticates the source nodes and the base station (BS). Also, BEARP designs the routing path selection system (RPSS) that includes the multiple-threaded process mechanism, and intrusion detection system (IDS) for security provisioning. BEARP mitigates the loads of sensor nodes by transferring routing related tasks to BS to improve the security mechanism performed uniquely by the secure BS. Moreover, it helps in maintaining network-wide energy equivalence and prolongs the network lifespan in WSN. In RPSS,
the BS periodically selects a newly best path from many paths based on the current energy level of nodes along each path. In the process of selecting the route, the algorithm multi shortest path is designed to create another child thread, which executes the function send route in time when finding a route to the source node. This thread is important to decrease the delay for sending routing information. To initiate the neighbor discovery, the BS selects a broadcast key to encrypt the packet neighbor discovery and broadcasts the packet confidential neighbor discovery (CND) to the entire network. Through the process of receiving, decrypting, segmenting, encrypting, and rebroadcasting the packet confidential, each node knows its real neighbor and stores it for use in the following phases. The BS waits for a short time to ensure that the packet confidential neighbor discovery broadcast can be flooded through the network. Then, the BS broadcasts another packet confidential neighbor collection (CNC) to collect the neighbor information of each node. On the receiving of CNC, sensor nodes flood a confidential neighbor collection reply (CNCR) packet to the BS. To select a path that has the maximum available energy on each node, the BS constructs a directed graph marked weight with neighbor information. The weight decreases as the head node sends and receives packets. The neighborhood matrix is proposed to represent the neighborhood relations between nodes. In the routing discovery phase, three subtasks are divided by the BS: (a) data enquiry, (b) routing path selection system (RPSS), and (c) sending routing information. The BS broadcasts confidential data enquiry (CDE) and waits for a reply for satisfied enquiry response, i.e., confidential data enquiry reply (CDER) from the sensor nodes. Once the BS has defined the routing path to the source, it forwards the confidential RR (CRR) packet. When the source node receives the CRR, the authentication process is performed. At the same time, using the path transferred with the CRR packet, it returns ACK packet to the BS to confirm the CRR delivery. After sending the ACK packet, source node transmits the real data. In the route maintenance phase, it is still the BS that works as the server to operate IDS and to release control information. The BS detects any compromised node which possibly exists in the network by impersonating regular users and sending each node arbitrary route requests one by one. All routing paths are selected uniquely by the BS, which defends adversaries to join in the WSN. Figure 20 shows the interrelated phases in BEARP.
When an adversary captures a sensor node in WSNs and knows all its secret keys, BEARP also has two methods for secure process: (i) routing paths selected uniquely by the secure BS, which reject a sensor node captured to imitate BS and (ii) IDS of detecting compromised nodes, which can take the sensor node captured out of the WSN. In intrusion detection systems, detecting compromised nodes is also performed uniquely by the secure BS. Hence, BEARP can effectively resist selective forwarding, wormhole, sinkhole attacks, and even a node captured. However, BEARP still designs the routing path selection system, intrusion detection system, and the multiple-threaded process mechanism. Since the secure BS performs the security mechanism uniquely, one aspect of sensor networks that complicates the design of a secure routing protocol is inside attacks, which result in vulnerability of the BS. Therefore, the burdening task on the BS is ineffective to support security for WSNs.

7. Discussion

In Table 2, we provide a comparative study of the secure multipath routing protocols based upon their security aspects. The evaluated metrics include the multipath technique and the additional security mechanism. In order to generalize the previous analysis, it also identifies the security requirements and specifies which protocol addresses which WSN attacks. In addition to security, the efficiency analysis is also presented. We have introduced an overview of tolerant-based, prevention-based, and mixed-mode approaches to secure multipath routing for WSNs. Each category has different goals in responding to the attacks on WSNs; therefore we should be vigilant about selecting the appropriate approaches.

Since node and link failure are persistent in data routing, the primary objective of the first category of protocols is to limit the effects of intruders and tolerates several types of routing attacks through relying on the benefits of the multipath method to provide secure data transmission in WSN. Different protocols have dissimilar multipath settings with different additional security mechanisms. For instance, the integration of N-to-1 multipath discovery protocol, hybrid multipath data collection scheme with the secret sharing in H-SPREAD scheme provides confidentiality and availability in data routing. Furthermore, cryptographic support in INSENS, enhanced INSENS, and MVMP are capable to fulfil the security requirements whilst, the others are partially achieve those requirements. Moreover, all protocols in this category have similarities in their effectiveness to inspect one type of attack namely spoofing, altering, and replaying routing information. MVMP only focuses on this single type of attack while the rest are able to tolerate few types of attacks. For instance, in SEIF routing protocol, each sensor should discover its reachable neighborhood, consisting of neighbors having a bidirectional link to defend against a HELLO flood attack. In terms of efficiency, while H-SPREAD is not focused on energy issues, all the protocols relied on this class are high in reliability. The analysis shows that H-SPREAD can achieve significantly better reliability and security seamlessly. INSENS and enhanced INSENS provide considerably low delay and overhead due to the employment of multiple base stations. MVMP has shown that the multi version of adopted algorithms has low computational complexity, low energy consumption, and reasonably high security. SEIF relies on one way hash chains to secure the construction of a multi-path dissemination tree and guarantee authentication of exchanged control messages without incurring high energy consumption.

From the proposed matrix, the prevention-based shows that SEEM and HSNRP have considered the shortest path algorithm in
Table 2
Comparison of the secure multipath routing protocols.

<table>
<thead>
<tr>
<th>TOLERANT-BASED APPROACH</th>
<th>PROTOCOLS</th>
<th>MULTIPATH TECHNIQUE</th>
<th>ADDITIONAL SECURITY MECHANISM</th>
<th>SECURITY REQUIREMENTS&lt;sup&gt;a&lt;/sup&gt;</th>
<th>RELATED ATTACKS&lt;sup&gt;b&lt;/sup&gt;</th>
<th>EFFICIENCY ANALYSIS&lt;sup&gt;c&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CD</td>
<td>IG</td>
<td>AC</td>
</tr>
<tr>
<td>INSENS (Deng et al., 2006)</td>
<td>Redundant multipath routing</td>
<td>Multiple base stations</td>
<td>Cryptography</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Enhanced INSENS (Deng et al., 2006)</td>
<td>Multipath routing to multiple base stations</td>
<td></td>
<td>Cryptography</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>MVMP (Ma et al., 2007)</td>
<td>Multiple data delivery paths</td>
<td></td>
<td>Data segmentation</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>SEIF (Ouadjaout et al., 2008)</td>
<td>Multipath selection scheme</td>
<td></td>
<td>Distributed and in-network execution which is designed based on the concept of one-way hash chains</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>PREVENTION-BASED APPROACH</td>
<td>PROTOCOLS</td>
<td>MULTIPATH TECHNIQUE</td>
<td>ADDITIONAL SECURITY MECHANISM</td>
<td>SECURITY REQUIREMENTS&lt;sup&gt;a&lt;/sup&gt;</td>
<td>RELATED ATTACKS&lt;sup&gt;b&lt;/sup&gt;</td>
<td>EFFICIENCY ANALYSIS&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CD</td>
<td>IG</td>
<td>AC</td>
</tr>
<tr>
<td>SEEM (Nasser and Chen, 2007b)</td>
<td>Modify the Breadth First Search (BFS) algorithm to get the relatively shortest path from the base station to source node</td>
<td></td>
<td>Lightweight broadcast authentication</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>HSNRP (Abid et al., 2009)</td>
<td>Shortest path algorithm</td>
<td></td>
<td>One-way hash chain</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>STAPLE (Gui et al., 2009)</td>
<td>Transmitting data to multiple parents</td>
<td></td>
<td>Public key Crypto System</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>EENDMRP (Gaurav et al., 2012)</td>
<td>Proactive node disjoint multipath routing protocol based on the rate of energy consumption and filled queue length of the node</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>mEENDMRP (Sangeetha and Yuvaraju, 2012)</td>
<td>Multipath routing and transmission range adjustment of the nodes in the paths</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOLERANT-BASED APPROACH</td>
<td>ADDITIONAL SECURITY MECHANISM</td>
<td>SECURITY REQUIREMENTS</td>
<td>RELATED ATTACKS</td>
<td>EFFICIENCY ANALYSIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTOCOLS</td>
<td>MULTIPATH TECHNIQUE</td>
<td>SECURITY REQUIREMENTS</td>
<td>RELATED ATTACKS</td>
<td>EFFICIENCY ANALYSIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTOCOLS</td>
<td>MULTIPATH TECHNIQUE</td>
<td>SECURITY REQUIREMENTS</td>
<td>RELATED ATTACKS</td>
<td>EFFICIENCY ANALYSIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeRINS (Lee and Choi, 2006)</td>
<td>Alternate path scheme</td>
<td>Neighbor Report System</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>N/A Med Med N/A</td>
<td>High Low Low High</td>
<td></td>
</tr>
<tr>
<td>PRSA (Al-Wakeel and Al-Swailemm, 2007)</td>
<td>Path redundancy based security algorithm</td>
<td>Various transmission modes</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>Redundant Round robin Selective</td>
<td>High Low High</td>
<td></td>
</tr>
<tr>
<td>SELDA (Ozdemir, 2007)</td>
<td>Secure multi path data transmission algorithm</td>
<td>Novel trust development algorithm</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>Web of trust</td>
<td>N/A Med Med High</td>
<td></td>
</tr>
<tr>
<td>SCMRP (Kumar and Jena, 2010)</td>
<td>Cluster based multipath</td>
<td>Cryptographic algorithm</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>Hash function</td>
<td>Low Low Low High</td>
<td></td>
</tr>
<tr>
<td>MSR (Moustafa et al., 2011)</td>
<td>On-demand multipath routing</td>
<td>Enhanced PACK</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>Erasure coding</td>
<td>Med Low Low High</td>
<td></td>
</tr>
<tr>
<td>SeMuRa (Triki et al., 2012)</td>
<td>Secure on-demand multipath routing</td>
<td>Watchdog mechanism</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>Uses labels in the datagrams exchanged to carry the threshold</td>
<td>Med Med Med High</td>
<td></td>
</tr>
<tr>
<td>BEARP (Zhou, 2013)</td>
<td>Algorithm multi-shortest path of the RPSS</td>
<td>Encryption and authentication IDS</td>
<td>CD IG AC AV SP SF SH WH SY HF EC DL OV RL</td>
<td>Routing paths selected uniquely by the secure BS</td>
<td>Low Low Low High</td>
<td></td>
</tr>
</tbody>
</table>

N/A: Non-Applicable.

Security Requirement: Confidentiality (CD), Integrity (IG), Authentication (AC), Availability (AV).

Attacks: Spoofing, Altering, and Replaying Routing Information (SP), Selective Forwarding (SF), Sinkhole (SH), Wormhole (WH), Sybil (SY), HELLO Flood (HF).

Efficiency Analysis: Energy Consumption (EC), Delay (DL), Overhead (OV), Reliability (RL), Medium (Med).
their routing schemes. However, SEEM did not employ other security mechanism in its routing scheme which reflects that the multipath itself can be used not only to support fault tolerance, but also security checking. Meanwhile, HSNRP uses a lightweight mechanism such as the broadcast authentication using the integration of μTESLA and bloom filters, μTESLA provides an authenticated broadcast for severely resource-constrained environments. However, their system requires synchronized clocks for all the nodes in the network. Bloom filters are space efficient data structures for membership addition and query, stored by all sender and receiver nodes. They store a set of entries to support membership queries, with a zero false positive rate and minimum false negative rate. Also, STAPLE transmits data through multiple parents to provide redundancy in data routing and uses the simple one-way hash chain to provide security in the routing procedure. EENDMRP and mEENDMRP have employed disjoint multipath routing with certain parameters and rely on pure cryptography system to enhance the security performance of their multipath routing protocol. STAPLE only focuses on selective forwarding attacks whilst the rest have shown their ability to prevent various types of WSN attacks (e.g., wormhole and Sybil attacks). Most of the protocols in this category provide high reliability in their routing performance. In terms of energy consumption, SEEM provides moderate performance in terms of the energy consumption since the sink node needs to update the information of the whole network topology, whilst the rest of the protocols show better energy consumption. HSNRP reduces the communication overhead over the expense of storing BF at both sender and receiver end, with compression and decompression requirements. STAPLE provides low energy consumption, delay, and overhead. The EENDMRP shows high overhead due to the pure cryptographic solutions in their routing protocols, whilst the modified version of EENDMRP reduces the unnecessary high transmission range of a node to increase the lifetime of the WSN and minimize the overhead.

The mixed-mode approach may consist of tolerant, detection, and prevention support in its routing scheme. It is beneficial for the secure multipath routing since it provides higher-level security. However, it may be inefficient for some applications as it applies a variety of techniques in order to satisfy the security requirements. SeRINS uses an alternate path scheme and neighbor report system to provide security in its routing operation. It performs detection support via the neighbor report system where a node’s route advertisement is verified by its surrounding neighbor nodes, and thus the suspected node is reported to the BS before being excluded from the network. PRSA only considers path redundancy based on the security algorithm by defining certain parameters to detect the presence of attacks and enhance the security through a various transmission modes. SELDA achieves security through the secure multipath data transmission algorithm. The backbone of SELDA is based on trustworthiness of sensor nodes and data aggregators. Also, it employs the watchdog mechanism for detection support. SCMRP is designed based on clustering and multipath concepts. It uses a pair wise key and unique shared key to distribute the routing information, so it is very difficult for an adversary to launch malicious activities. There are two protocols in this class using an on-demand platform for their routing operation; namely MSR and SeMuRa. Enhanced PACK helps to enhance the security and attacks detection in MSR. Meanwhile, the on-demand properties in SeMuRa allow this protocol to specify the path-disjointness threshold value. While updating the list of paths in use if the network topology changes, the intermediate nodes use the watchdog concept for every packet they forward to detect the identities of misbehaving nodes or routes errors. SeMuRa adopts a signature scheme to authenticate nodes and guarantee the integrity of the information they exchange. BEARP based on the concept of shortest path algorithm and unique base station where the routing paths are selected by the secure BS. It also encrypts all communication packets and authenticates the network entity such as source nodes and the base station. The routing path selection system, intrusion detection system, and the multiple-threaded process mechanism for BEARP are still in the design phase. SCMRP, and BEARP satisfy all the security requirements of WSNs, whilst PRSA and SCMRP fulfill all the security attacks attributes. For instance, BEARP has achieved all of the security requirements via the implementation of multipath routing, which consists of two methods for secure process: routing paths selected uniquely by the secure BS and IDS for detecting compromised node as well as the encryption and authentication mechanisms. SCMRP and BEARP show a favorable performance in terms of efficiency (e.g., node packet delivery ratios and network lifetime) even in the presence of compromised nodes. For instance, the design of BEARP not only increases the speed of selecting a path to the source but also saves the memory space. SeRINS concern with security results in medium delay and overhead especially in large networks. PRSA shows high energy consumption due to the usage of various transmission modes. Although the delay and overhead is at the medium level, the reliability of the whole protocol performance is high in SELDA. The combination of on-demand routing with enhanced PACK and erasure coding minimize the delay and overhead in MSR. Meanwhile, the intermediate verification of packet signatures allows discarding compromised packets before they reach the destination nodes, which optimizes the energy used and communication resources and reduces the overhead of the signature verification process performed by the BS in SeMuRa.

We can conclude that the multipath approach can be used not only to support fault tolerance, but also security checking and provides high reliability in data routing. In terms of the security mechanisms, cryptography algorithm is the most popular approach to be integrated with multipath routing in achieving security in a sensor network routing protocol. With careful design of the routing technique, this heavyweight mechanism shows a better performance in security such as that performed by SCMRP. Broadcast authentication mechanism is also used by two types of routing protocols namely, HSNRP and SeRINS to defend against WSNs attacks. In HSNRP, μTESLA provides an authenticated broadcast for severely resource-constrained environments. However, their system requires synchronized clocks for all the nodes in the network. Bloom filters are space efficient data structures for membership addition and query, stored by all sender and receiver nodes. They store a set of entries to support membership queries, with a zero false positive rate and minimum false negative rate. They reduce the communication overhead over the expense of storing BF at both sender and receiver end, with compression and decompression requirements. In SeRINS, ARMS is employed for broadcast authentication of the sensor node’s route advertisements, with a small memory space, and no clock synchronization. It also mitigates the effect of packet loss. One drawback of ARMS, however, is that it has a total of 20 extra bytes added to routing information. The basic idea of ARMS is that a broadcast sender makes consecutive broadcast packets uniquely related and receivers authenticate broadcast packets immediately by verifying that relation, which can be defined by a public one-way hash function. ARMS prevents a routing message from being spoofed and altered, by means of a one-time key MAC scheme. In addition, SeMuRa adopts the watchdog technique to detect nodes that do not forward the
datagrams as expected. A node which uses the watchdog technique is able to determine whether its neighbor nodes are forwarding the datagram they receive or vice versa.

Based upon the proposed matrix, authentication and availability are the most satisfied security requirements among the selected protocols. Therefore, the protocols that address these requirements can resist the typical WSN attacks such as spoof, alter, or replay routing information and selective forwarding. The conclusion drawn is that multipath routing is sufficient to counter certain types of attacks and it should be designed on a case-by-case basis to minimize the impact of WSN threats throughout the entire protocol. With the integration of additional security infrastructure, this research has highlighted a number of multipath protocols that provides some degree of protection during the data communication phase of the sensor network.

8. Conclusion

In WSNs, the data transmission is still vulnerable to various attacks. Some solutions have been proposed by the research community to counter these attacks without using security mechanisms and others with additional security mechanisms, but most of the protocols only defend against certain types of WSN attacks. To design a protocol that can reduce the impact of potential security attacks on WSNs, an essential step would be to review the available solutions for protecting data communication and the numerous types of security threats. The objective would also be to obtain an optimum solution with none of the drawbacks or limitations observed for previously developed solutions. Hence, the multipath technique can be improved by designing it on a case-by-case basis in multipath algorithm. For future work, in order to validate the proposed architecture, the aim is to design and develop the aforementioned solution. Moreover, a lightweight defense mechanism can also be integrated into multipath routing to deal with the limitations posed by WSNs.

Acknowledgment

This research was financially supported by the Ministry of Education (MOE) Malaysia. In addition, the authors would like to thank Universiti Tun Hussein Onn Malaysia (UTHM) for sponsoring the research work. The authors wish to thank the reviewers and editor who have improved the paper very significantly.

References


