A Study of Secure Routing Protocols for Wireless Sensor Networks

Reem Abu Taleb
Department of Management Information Systems, Business Faculty, Al Balqa’ Applied University, Jordan
reem_abutaleb@yahoo.com

ABSTRACT

Wireless sensor networks are usually deployed in inhospitable environments in order to accomplish a specific mission. As a result, these networks are subject to various numbers of attacks and threats. Therefore, security should be a major aspect that must be taken into account when designing routing protocols for wireless sensor networks. Additionally, sensor nodes have limited resources. Thus, complex routing and security protocols cannot be used. In this paper we provide a survey of secure routing protocols that can be used in wireless sensor networks since it is important to provide a classification of the available protocols. Therefore, several protocols were reviewed in this paper. The routing protocols can be classified into two main categories namely topology based and protocol operation based. The main goal of the work proposed in this paper is to provide researchers with a clear idea about the available security based routing protocols and their properties.

Keywords: Wireless sensor networks, Security, Routing, Hierarchical, Base Station, Sink

1. INTRODUCTION

Advances in wireless communications and electronics have made it possible to manufacture small and light weight sensor nodes that can be densely deployed in various environments in order to achieve certain goals by forming a wireless sensor network (WSN). As a result, WSNs have become an interesting area of research due to their various areas of applications such as industrial, agricultural and military applications [1-8].

Sensor nodes have limited life time because they are battery operated. Moreover, sensor nodes consist of three subsystems namely, computing subsystem, sensing subsystem and communication subsystem. Furthermore, the amount of energy consumed by the communication subsystem is much higher than that consumed by the computing subsystem and is dependent on the transmission distance and attenuation. Therefore, several techniques have been proposed in order to reduce the amount of energy consumed by the communication subsystem to prolong the life time of sensor networks [9-14].

As a result, several routing protocols have been proposed in order to prolong sensor nodes’ lifetime. These protocols mainly rely on multihop routing in order to reduce the transmission distance and extend network life time. Hence, routing protocols for WSNs can be classified into two main categories namely Topology Based and Protocol Operation Based. These two main categories can be further subdivided into subcategories. Routing protocols that can be classified as topology based rely on information regarding existing links in the network in order to forward packets. On the other hand, protocols that can be classified as operation based have routing approaches that depend on the routing mechanism used. Furthermore, operation based routing protocols work according to the operation of the network structure. In other words, these protocols work according to sudden changes that may occur and affect the network structure [15][16].

Since routing protocol for WSNs use multihop routing, there is an increasing need for adopting security mechanisms in order to achieve both security and energy efficiency requirements. However, sensor nodes have limited energy. As a result, cryptographic algorithms that rely on using public key such as RSA and Diffie-Hellman are complicated and energy consuming to be used in WSNs. On the other hand, the symmetric key cryptographic technique is favored on public key cryptography due to its own qualities. In addition, several aspects have to be taken into account such as encryption keys establishment, key distribution and key management, in order to provide security mechanisms in WSNs.

Therefore, there is a profound need to balance between security levels required to mitigate security risks and the amount of energy consumed by the adopted security mechanisms [17]. Hence, several secure routing protocols are discussed in this paper.

The rest of this paper is organized as follows. In section 2 the security requirements in WSNs is studied. After that, types of Attacks that can be initiated against WSNs are reviewed in section 3. Also, a Secure routing protocols for WSNs are reviewed and classified in section 4. In section 5 a discussion regarding the studied protocols is provided. Finally, conclusions and future work are present in section 6.

2. SECURITY REQUIREMENTS IN WSNs

There are certain security requirements that must be met in order to deal with security issues that may occur in WSNs. In this section several security properties and implementation that may help to improve security levels in WSNs are discussed.

2.1 Authentication

Authentication gives sensor nodes, within a WSN, the ability to communicate and cooperate without risk through identifying and controlling nodes participating in the network. As a result, confidentiality
and integrity of exchanged messages is achieved when we make sure that data is communicated with the correct node from the start. Consequently, it is vital to provide the receiver with the necessary mechanisms to ensure that the received messages are indeed sent from the actual node within the WSNs. Thus, Message Authentication Codes (MAC) such as HMAC can be used to achieve both authentication and integrity of messages [17][18].

2.2 Availability
The service provided by a WSN should be available all the time even in the presence of internal and external attacks. As a result, a central access control system is required to make sure that every message has been delivered successfully to its intended recipient [17].

2.3 Data Confidentiality
It is very important to make sure that messages communicated between the sender and the receiver are kept confidential. Thus, if an authentic node is not the intended recipient of a message, that node must not be able to see the contents of that message. In other words, a sensor node that has been authenticated to participate in a WSNs, must not be able to check the contents of a message unless the message was sent to that node. Therefore, several cryptography keys such as symmetric and asymmetric keys can be used to achieve confidentiality [17].

2.4 Data Integrity
It is very important to make sure that the contents of messages cannot be modified by an entity while messages traverse the network in order to reach their intended recipients. Therefore, several cryptographic techniques can be used in order to achieve data integrity such as MD5 and Secure Hash Algorithm-1 (SHA-1) [17][19].

2.5 Data Freshness
It is essential to make sure that data communicated between participant nodes in WSNs is up-to-date. Additionally, there is a need to guarantee that no adversary take advantage of old messages in order to initiate attacks. It is important to ensure the freshness of data for sensor nodes especially when shared keys are used to communicate messages because a reply attack using the old key can be initiated by an adversary [17].

2.6 Self-Organization
Since WSNs topology is highly dynamic, Self-Organization is one of the main properties of WSNs. However, this property imposes a security challenge for WSNs. Therefore, deploying any preinstalled shared key mechanism might be impossible. Thus, it is vital that sensor nodes self-organize themselves not only for multihop routing but also for key management and for the development of trust relations [17].

3. TYPES OF ATTACKS IN WSNs
According to [20] there are several attacks that can be initiated against WSNs. Some of these attacks are listed and discussed in this section.

3.1 Sinkhole Attacks
In this type of attack, the network traffic is attracted through a compromised node by the adversary. Consequently, this type of attacks can be initiated by placing the malicious node in a position where it is capable of attracting most of the traffic in the network. In other words, the malicious node could be placed near the base station or it can be acting as a base station. As a result, all or most of the traffic has to pass through the malicious node or might be destined to the malicious node. Furthermore, this type of attacks applies selective forwarding in order to make the network traffic go through the malicious node [21].

3.2 Hello Flood Attacks
This attack is based on broadcasting HELLO messages with strong transmission power and pretending that these messages are being transmitted by the base station. Note that, these HELLO messages are sent with strong transmission power so that the message can reach the largest possible number of sensor nodes in the network. After the HELLO message is received by the sensor nodes, the receiving nodes will assume that the source of the HELLO message is closest node to the base station. As a result, all the traffic generated by these nodes will pass through the node that has sent the HELLO message. In addition, sensor nodes will consume most of their energy responding to the flooded HELLO messages which affect the network life time. Also, HELLO messages will be broadcasted by the base station but a small number of sensor nodes will be responding to it [21].

3.3 Wormholes
To initiate this attack, an adversary is placed close to the base station so that, the network traffic can be completely disrupted where a low latency link is used to tunnel messages. In this type of attacks sensor nodes that are multiple hops away from the base station are convinced that they are closer to the base station. As a result, a sinkhole is created because better routes to the base station can be provided by the other side of the sinkhole [21].

3.4 Sybil Attacks
In this type of attacks multiple illegitimate identities are created by the malicious node. Hence, the identity of a legitimate node is stolen or fabricated by the malicious node. In order to reduce the capabilities and effectiveness of fault tolerant techniques Sybil attacks can be initiated against routing algorithms and topology maintenance. Moreover, Sybil attacks can be used against geographic routing where the malicious node appears in multiple places simultaneously [21].
3.5 Selective Forwarding

This type of attack is considered as a way of affecting the network traffic by making all authentic sensor nodes believe that all nodes participating in the network are authentic and are reliable to be used to forward messages. In this attack, certain messages are dropped, by the malicious node, instead of being forwarded. Thus, once a message is received by the malicious node, the malicious node reduces the latency in order to deceive its neighbors and to convince them that they are not on the shortest path. Worth mentioning, the efficiency of the selective forwarding attack is dependent on two elements namely the location of the malicious node and the percentage of dropped messages. For the first element, the malicious node will be able to attract more traffic if it is placed closed to the base station. On the other hand, for the second element, when the malicious node drops a large number of messages and does not forward them it can conserve its own energy and prolong its life time in order to remain powerful to continue the attack and deceive its neighbors [21].

3.6 Denial of Service Attack

This type of attacks can be initiated at the physical level using different techniques such as radio jamming, interfering with the network protocol and depleting sensor nodes batteries [21].

4. SECURITY PROTOCOLS CLASSIFICATION

Since sensor nodes have limited energy sources, multihop communication is used to route messages from source to destination in order to reduce the amount of energy consumed in transmission. As a result, routing protocols are considered as a fundamental part of the network in order to be able to deliver messages to their intended recipients. Thus, sensor nodes act as sources of data and as routers to forward messages originating from other sensor nodes in the network.

Because messages have to go through multiple nodes in order to reach their destination, WSNs are susceptible to various types of attacks that were discussed in section 3. Additionally, the limited energy of sensor nodes affects the topology of the network. In other words, because some nodes in the network might suffer from energy depleting, the topology WSNs is highly dynamic. Therefore, routing protocols proposed for WSNs must take these issues into account and try to provide the required security levels along with being able to tolerate various changes in the topology that might occur during the network life time.

Many secure routing protocols for WSNs have been proposed and they can be divided into two main categories topology based and protocol operation based. The first category uses information about the existing links in the current topology in order to forward messages. However, routing protocols that fall under the second category adapt to changes that may occur in the network structure to keep the network functional and achieve the required performance levels [15][16][22].

Topology based routing protocols can be further divided to flat network routing, hierarchical network routing and location based routing. On the other hand, protocol operation based routing category can be divided into negotiation based routing, multipath based routing and query based routing, see figure 1 [15][16][22].

In this paper we will study some protocols that fall under the first category while a brief explanation of the second category is included.

![Fig 1: Protocols Classification](image)

4.1 Topology Based Routing Protocols

The network structure and topology play a major role in the operation and performance of routing protocols used to deliver messages in WSNs. Topology based routing protocols can be divided into flat network routing, hierarchical network routing and location based routing. In this section protocols that fall under this category are discussed.

4.1.1 Flat Network Routing

Routing protocols in this category give sensor nodes equal roles in terms of sensing and communication in order to report the collected information to the base station [16][22]. The Localized Encryption and Authentication Protocol (LEAP) was proposed in [23] where each sensor node establishes four types of keys in order to communicate with other nodes in the network. In this protocols, the established keys can be used for different purposes. A sensor node establishes an individual key and share it with the base station in order to communicate with it. Furthermore, a pair wise key is used to communicate with other sensor node in the network. Also, a cluster key is used by a sensor node to communicate with its neighbor. Finally, a group key is assigned for all sensor nodes participating in the network. Worth mentioning, these four keys are updated periodically in order to maintain a certain level of security [23].

Another secure routing protocol for WSNs called SPINS was proposed in [24]. SPINS consists of two main optimized security building blocks namely SNEP and µTESLA. The baseline security primitives such as data
confidentiality, two-part data authentication and data freshness are provided by SPEN. On the other hand, authenticated broadcasting is provided by µTESLA [24].

Another secure version of SPIN that is called Secure SPIN (SSPIN) was proposed in [25]. In order to provide message integrity and data correctness Message Authentication Code (MAC) algorithms are used. Moreover, the operation of SSPIN can be divided into three stages; an ADV message is created using the MAC algorithm when a sensor node has a new data to be sent.

When the receiving node obtains the ADV message it verifies it using the MAC algorithm. After that, a REQ message is sent to the source of the ADV message who verifies the REQ message using the MAC Algorithm. Finally, DATA communication is started if the REQ message is valid [25][26].

The authors in [27] have proposed an Energy-Efficient Secure Routing Protocol (EESRP) to provide security and energy efficient mechanisms for WSNs. The proposed protocol consists of two main parts. The first part is Roulette-Wheel Routing Protocol (RWRP) that is used to forward messages from source to destination where the forwarding decision are taken independently by each node without the need for collecting information from other neighboring nodes . The second part is Secure Routing Protocol (SRP) that is concerned in securing messages until they reach their intended recipients. In SRP µTESLA is used to authenticate messages originating from the sink node. Additionally, confidentiality, authentication, integrity and data freshness are provided using MAC algorithms and time stamps [26][27].

4.1.2 Hierarchical Network Routing

Routing techniques that are classified as hierarchical protocols are based on dividing nodes in the network into groups or clusters where each cluster has its own cluster head. In order to reduce the amount of energy consumed in communication and processing, the cluster head is responsible for collecting and aggregating data.

Moreover, it is the cluster head’s responsibility to check for data redundancy before reporting the collected information to the base station [16][22].

Many routing protocols have been proposed to secure the operation of hierarchical WSNs, in this section some of these approaches are reviewed.

An energy efficient cluster based key management protocol (EECBKM) has been proposed in [28]. In this protocol, cluster heads are selected based on energy cost, coverage and processing capacity. After that, the base station assigns an EBS key set and a cluster key to every cluster head and cluster respectively. For inter-cluster and intra-cluster communication the EBR key set is used as it contains the pair-wise keys. In addition, the cluster head is responsible for distributing the keys to sensor nodes in its cluster. Thus, secure channels between sensor nodes and the cluster head can be established after key distribution is accomplished [17][28].

To provide energy efficient and secure communication, a secure hierarchical energy efficient routing protocol (SHEER), was proposed in [29]. The proposed protocol is based on using hierarchical key establishment system and a probabilistic transmission mechanism in order to improve the network energy performance and prolong the network life time [17][29].

Sec LEACH which is a protocol for securing clustered wireless sensor networks was proposed in [30]. The proposed protocol uses random key pre-distribution and introduce the use of symmetric key and one way hash chain. Thus, different performance numbers regarding efficiency and security can be provided [17][30].

In order to provide acceptable security services for cluster based WSNs, a novel secure key management module for hierarchical wireless sensor networks (NSKM) was proposed in [31]. The proposed scheme uses a pre-deployed keys, network generated keys and a base station broadcasted keys. Moreover, the selection of a secure cluster head from all the available cluster heads is based on the cluster head’s location and distance from the base station [17][31].

The authors in [32] proposed a secure hierarchical model for sensor networks (SRPSN). In order to protect data, all cluster heads and the base station share a preloaded symmetric key. Also, SRPSN is based on a group key management scheme that includes policies for group communication, requirements for group membership and group key generation and distribution algorithm. Worth noting the partial key of every sensor node is used in order to compute the group key [17][32].

4.1.3 Location Based Routing

The operation of location based routing protocols relies on addressing each sensor node using its location. Worth mentioning, the position and location of sensor nodes is calculated according to the signal strength received from a node [16]. Several routing protocols can be classified under this category and some of these protocols are discussed in this section.

The research presented in [33] proposed a secure position aided ad hoc routing protocol (SPAAR). The main goal of SPAAR is to protect location related information of sensor nodes. Furthermore, the protocol makes use of nodes location information in order to take routing decisions. Thus, the number of control messages regarding routing is reduced.

In this protocol, every node is required to have public and private key pair along with a certificate to bind its identity to the public key. Furthermore, a table update message is broadcasted by every sensor node periodically in order to inform its neighbors regarding its position,
since each node maintains a table regarding its neighbors and their location information [15][33].

An anonymous on-demand position-based routing in mobile ad hoc network (AODPR) was presented in [34]. AODPR aims to prevent any possible traffic analysis by keeping routing nodes anonymous. A node is required to register with a position server. As a result, a common key and public/private key pair are obtained from the position server. Furthermore, when a node needs to get position information regarding other nodes in the network, it is required to authenticate itself and send a signed request to the position server.

Consequently, the position server replies by sending the required information to that node. In order to improve security levels in the network, position information are encrypted using the common key. Thus, position information cannot be accessed from nodes that are not participants in the network [15][34].

The research proposed in [35] presented a Secure Position-based Routing Protocol for Mobile Ad Hoc Networks (SGF). Shared key and the instant key disclosure (TIK) are used to provide source authentication, neighbor authentication and message integrity. The mechanism of SGF combines the use of the hash message authentication code (MAC) with the timed efficient stream loss tolerant authentication (TESLA) along with TIK protocol. The SGF makes use of a reputation system that provides that ability to classify nodes as good or bad. As a result, message tampering and attackers can be detected and dropped respectively [15][35].

4.2 Protocol Operation Based Routing

The protocols that fall under this category work according to the current network topology and can adapt to changes in topology that might occur during the network life time. This category can be further divided into negotiation based routing, multipath based routing, query based routing and quality of service based routing [16].

4.2.1 Negotiation Based Routing

Negotiation based routing protocols use high level descriptors as a result redundant data transmission is eliminated [16]. Also, decisions regarding communication are made based on the available resources for the sensor nodes. SPIN protocol family is negotiation based protocols. In section 4.1.1 SPINS and SSPIN have been discussed.

4.2.2 Multipath Based Routing

Routing protocols under this category improve the network performance by using multiple paths instead of using a single path to deliver messages to their destinations. These protocols are considered to be fault tolerant because multiple paths are used which helps to increase the network life time. Furthermore, the more paths available between nodes the higher the fault tolerance capabilities of the network [36].

4.2.3 Query Based Routing

In this type of protocol, the sink nodes of the base station send sensing tasks for sensor nodes, and the sensor node or nodes that have data matching the received query send the required data to the node that have sent the query in the first place [36].

4.2.4 Quality of Service based Routing

This type of routing protocol concentrates on the quality of data and the energy consumption of sensor nodes. As a result, certain quality of service parameters must be met whenever data is requested from a sensor node [16].

5. DISCUSSION

In this paper several secure routing protocols for WSNs were discussed. As mentioned before, routing protocols can be divided into topology based and protocol operation based. In this paper our main focus was at the topology based routing protocols and several protocols that fall under this category were discussed.

The first sub category discussed is flat based routing protocols. The first routing protocol discussed is LEAP. This protocol provides security for WSNs using four different types of keys. However, using four different keys makes the computation very complicated and needs more storage space if compared with other techniques. Additionally, there is an overhead incurred from using these keys and when exchanging and updating them which may affect the network life time.

Many security issue were addressed by the SPIN family protocols. However, the discussed protocols do not completely deal with compromised nodes. Also, the discussed protocols are not capable of dealing with the denial of service attack [37]. The last protocol discussed under this sub category is EESRP, which capable of providing protection against most of the attacks discussed in this paper [27].

For hierarchical routing protocol, EECKBM was discussed. EECKBM is capable of reducing node capture attack. Furthermore, this protocol has efficiently increased packet delivery ratio [17].

SHEER protocol is able to defend against hello flood attack, Sybil attack and sinkhole attack. On the other hand, this protocol fails to defend the network against selecting forwarding attacks [17]. The Sec LEACH protocol is capable of reducing the total energy consumption in the network. Thus, the network life time was prolonged [17].

NSKM protocol makes sure that the whole network is never compromised even though an attack might be initiated against the network. Furthermore, this protocol is lightweight and scalable. Thus, it is suitable to be used with large WSNs [17].
The last protocol discussed in this sub category is SRPSN. This protocol was designed to secure data transmission under different types of attacks. On the other hand, this protocol does not have authentication mechanism. Thus, it fails to protect the network from attacks such as Sybil attack [17].

For location based routing protocols, SPAAR protocol was discussed. this protocol provides the needed requirements to ensure secure routing using asymmetric cryptography to protect the network from malicious nodes. On the other hand, it has medium scalability because the existence of a certificate server is required which causes a bottleneck to appear in the network. Furthermore, this protocol suffers from high packet overload and high probability of long routes especially when the number of nodes in the network is large [15].

AODPR has a high probability of using the optimal path. Also, loop-free operation is guaranteed because this protocol used sequence numbers and depends on forwarding packets to nodes towards the destination. However, there is a big concern that the key will be kept uncompromised especially when large number of communications is carried out using the common key [15].

Source authentication, neighbor authentication and message integrity are provided by SGF. In addition, SGF is capable of tolerating position inaccuracy generated by the list of neighbors HELLO message. On the other hand, this protocol is complex to be implemented since many security techniques are used during location service and forwarding process [15].

6. CONCLUSIONS AND FUTURE WORK

Sensor nodes have limited energy sources. As a result, routing protocols are vital to WSNs operation in order to energy efficient operation and prolong network lifetime. In addition, sensor network are deployed in hostile environments and are expected to operate in an unattended manner for long periods of time. As a result, security plays a major role in the network operation so that, correct information is reported by WSNs. Therefore, routing protocol must take into account different security threats and attacks that might initiated against WSNs when routing messages. Some secure routing protocols have been classified and discussed in this paper. Also, the operation of the listed protocols has been studied and their performance was discussed. Further research may be carried in order to study the effect of mobility and mobility models on the performance and security of the routing protocols discussed in this paper.

REFERENCES


AUTHORS
Reem Abu Taleb is a lecturer in the department of Management Information Systems at al Balqa’ Applied university. She received MSC Degree in Computer Science from al balqa’ applied university in 2007, BS.C degree in Computer science for the University of Jordan in 2000. Reem Abu Taleb has published several journal and conference papers. Her main research interests are security, wireless sensor networks and distributed systems