I.J. Wireless and Microwave Technologies, **2016, 3, 9-19**
Published Online May 2016 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2016.03.02

***Available online at* http://www.mecs-press.net/ijwmt**

A Survey on Secure Routing Protocols in Wireless Sensor Networks

Yasir Arfat, Riaz Ahmed Shaikh

Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Abstract

Wireless Sensor Networks (WSNs) are typically formed by the collaboration of the large amount of partial sensor nodes, which are connected through a wireless medium. In wireless sensor network, security is an essential aspect because of its usage in applications like monitoring, tracking, controlling, surveillance etc. Secure communication is extremely crucial in delivering vital information accurately and on the time through resource constraint sensor nodes. In this paper, our contribution is threefold. Firstly, we have summarized the network layer routing attacks on WSNs. Secondly, we have provided a taxonomy of secure routing protocols of WSNs. Thirdly, we have provided a qualitative comparison of existing secure routing protocols. Results show that most of the existing secure routing schemes are not very efficient due to various reasons like high-energy consumption, and large communication overhead.

Index Terms: Secure Routing, Cryptography, and Sensor networks, Geographical Routing.

1. Introduction

Wireless sensor network (WSN) consists of a large number of closely deployed sensors. There are various applications of WSNs like military, environment monitoring, surveillance, health care, and industrial monitoring. In WSNs, sensor nodes have limited storage, transmission range, network bandwidth, and energy. Due to resource constraint nature of sensor nodes, incorporating security features (e.g. encryption/decryption, authentication) is a challenging task. Depending on the security features, network performance (in terms of energy, memory, communication cost) can be degraded.

In wireless sensor network, it is highly possible that during the transmission of a data from source to the destination it can be eavesdropped, captured and altered [15]. Thus, the security of the critical infrastructure of wireless sensor network is crucial and needs to be protected.

Mostly, security issues in routing protocols do not get the copious attention and keeping the security in mind

* Corresponding author.
E-mail address: yasirarfat081@gmail.com

does not develop many routing protocols. In numerous applications, data is very essential; for example, if we are monitoring the weather forecasting using the WSNs, a malicious user can inject false information then the authentication of such information becomes a critical concern. Various researchers have adopted cryptographic approaches to avoid such attacks on the WSNs.

In this paper, we focused on secure routing protocols [1], [2], [6], [12] of WSNs. There are various security needs that a secure routing protocol should contain. For example,

- Sensor nodes need to collaborate with each other to avoid attacks,
- Sensor nodes need to communicate securely and data should be protected,
- Information sent over the network should not be altered or modified by an adversary during transmission,
- Availably of nodes should be ensured, and
- Identities of the sender nodes should be verified.

In this research paper, we classify the secure routing protocols into different categories based on security techniques and presented the taxonomy. Also, we have provided a qualitative comparison of the recent secure routing protocols of WSNs. We found out that researchers are applying the cluster and none cluster based cryptography approaches for the secure routing in WSNs. We also examined the existing techniques on the bases of their attributes such as, environmental and security assumptions, security approaches, protocol classification and protocol type.

The rest of the paper is organized as follows. Section 2 briefly describes the existing literature survey. Section 3 summarizes the network layer attacks. Section 4 presents a taxonomy of secure routing protocols. In section 5, we have provided a comparison of secure routing protocols. In section 6, we have discussed future challenges and issues. Finally, section 7 concludes the paper.

2. Literature Survey

This section presents an overview of the state-of-the-art secure routing protocols [1,2,4-14] of wireless sensor networks. This overview composed of discussion about the assumptions, methodologies, and key approaches present in existing works. Based on this section, we will present taxonomy and comparison in the following sections.

2.1. Light weight Secure-Low-Energy Adaptive Clustering Hierarchy (LS-LEACH) Routing Protocol

Alshowkan *et al.* [1] have proposed a Lightweight Secure-Low-Energy Adaptive Clustering Hierarchy (LS-LEACH) in which they firstly discourage the attacker to join the wireless sensor network using lightweight and energy-efficient authentication function in which the cluster head verifies the validity of nodes, which ask to join the cluster. Secondly, they described the threshold for the typical node-to-node number of connections through the time. This is used to detect the strange activities happened between nodes. Thirdly, they described the effective use of time division multiple access (TDMA) in the LEACH so that every node can only send data to the cluster head. They also described the mechanism to use LS-LEACH in WSNs by election, connection, and transmission in which different formulas are used. They assume that every node has two secret keys. One key is shared among all nodes, and it is also shared with the base station. When the node becomes a cluster head, then the private key will be shared with the base station. On the other hand, the group key is used to join clusters. They also assume that the number of cluster heads should not be more than 5% of total nodes. At the start of each subsequent cycle after network deployment, cluster head will be elected. They describe that wireless sensor network is facing lots of problems such as inadequate resources in energy, power consumption and storage. There is another challenge that the uniqueness of the broadcast medium makes the wireless sensor networks at risk to a number of attacks. An attacker can join the wireless sensor network and may seize, insert or broadcast the data. They compared the performance of LS-LEACH and LEACH using system throughput, lifetime of the network and the amount of energy they consumed.

2.2. Secure Geographical Routing (SGR)

Lata *et al*. [2] have presented the Secure Geographical Routing (SGR) algorithm for wireless sensor network to identify event and sends information to the base station. In previous approaches, there was a problem of transmitting multiple copies of the data packet through multiple paths that consumes energy instead of a single copy of data transmission. They assume that the base station is placed at the co-ordinates (0, 0) in the network region. The base station has unlimited energy. Each node is labeled with a distinctive ID. Based on the communication distance, nodes have the ability to adjust power. They described that the static and homogenous network model that works on "Collaborate, Collate and Compare" (CCC) formula. In that model cluster head gives and receives the information about its neighboring node. In the SGR algorithm, first GPS nodes were deployed along key with the value of x and y co-ordinates. In the second step, data will be collected. If the average value of the data is above than the threshold value, then data transmission will be started. In third and final step, Global and Local broadcast will be used. Local broadcast ensures delivery of data from one node to the next node securely; whereas, global algorithm ensures end-to-end connectivity between sender and base station. To improve the reliability, if an acknowledgment is not received, then again a copy of data will be transmitted from another path.

2.3. Design and Analysis of Secure Routing Protocol (D&ASRP)

Cheng *et al.* [3] have presented the design and analysis of secure routing protocol for wireless sensor networks (WSNs). A secure protocol is designed to deal with the DoS attack to the sensor network. Meanwhile, wireless sensor network have limited resources in terms of processing capability and memory. So the design focuses on reducing the cost upon increasing the processing capability and memory. In the proposed scheme they firstly describe a network model. A network model consists of a base station and sensor nodes, which can be grouped into a cluster. Each cluster could be divided into sub-clusters. Each cluster has a gateway, which is reachable to all sensors in the cluster. They also assumed that two nodes can possibly communicate from the transmission the distance. This assumption is based on a hierarchical routing algorithm; according to this requirement, every sensor node is able to adjust its transmission radius. The chosen algorithm for routing protocol adopts suitable routing technology based on the various factors such as, distance between nodes and the base station, the nodes distribution density and remaining energy of nodes. Analysis of the proposed scheme shows that the complexity of the algorithm is $O(N^2)$ and furthermore security analysis shows that the algorithm for routing protocol is secure and efficient for wireless sensor networks.

2.4. Secure Communication and Routing Architecture (SC&RA)

Khan in [4] has proposed the secure routing architecture for wireless sensor network. In that work authors assumed that the base station is located at the center of the network which provides better load balancing. Authors also assumed that all sensor motes (SMs) will be distinct, inactive, outfitted with resistant hardware and compute space by signal-strength. Cluster head will correspond to one another directly with the distinct secret key provided by the base station. The strategic method set security architecture in the design of routing protocol, in a spite of creating separate protocol for well-organized routing & interruption detection. It consists of three steps: cluster formation, route formation, and data forwarding. The cluster formation helps in less energy consumption in the network. In the route formation step, a routing is developed and all the sensor motes (SMs) forward their topology information to Cluster Head (CH) through the route response message. Data is forwarded using multipath routing table with a key pair that was shared by cluster head. Simulation results show that network setup takes less time, introduces less communication overhead and attacker success rate is also decreased.

2.5. Secure Energy efficient Secure Directed Diffusion Protocol (ESDDP)

Belkadi *et al*. [5] have presented the energy-efficient and secure directed diffusion protocol for wireless sensor network. Security and energy play an important role in wireless sensor networks (WSNs) for many daily life applications. They mentioned that many researchers do not consider both energy and security simultaneously in WSNs. The proposed secured directed diffusion protocol uses three types of keys. First, an individual key (IK) of a node, which is used, for secure communication among nodes and the base station. Second pair-wise key (Kpair) is used for secure communication among node and its neighbors and third global key (BK) that is distributed by the base station to all the sensor nodes. The base station uses BK to encrypt messages and every node in a network uses this key to decrypt the announcements from the base station. Authors did the performance comparison of the secured directed diffusion and directed diffusion. Results show that the secured directed diffusion protocol reduces the energy and increases the lifetime network.

2.6. The Trust-based Energy Efficient Secure Routing Protocol (TEESR)

Durrani *et al*. [6] have presented the trust-based energy efficient secure routing protocol (TEESR). They highlighted the challenges, routing security threats, requirements, and assessment of existing solutions. This protocol has a limited number of forwarding nodes, floods the neighbors information in a small amount of messages as compared with other routing protocols. Consequently, the proposed scheme reduces end-to-end delay and saves considerable energy. The design of trust-based energy efficient secure routing protocol (TEESR) contains three main advantages. First, this protocol restricts malicious nodes in its surrounding area by using suitable verification and flooding technique. Second, this protocol act upon resource intensive computations such as construct routing tables. Third, the protocol uses multipath overlay networks to exploit redundancy and bear intrusion in a specific area. This protocol has different phases like cluster formation phase, data forwarding phase. Each phase uses different NBRDET message formats for clustering and forwarding. They compared the performance in term of security, energy, the number of drop messages, and end-to-end delay with other routing protocols. The results show that the selected protocol has better performance.

2.7. Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP)

D'Souza *et al*. [7] have proposed the secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP). This routing protocol uses the multipath from source to destination based on less energy consumption and the queue length of a node. It also provides security against the attacks like sinkhole, and selective forwarding in WSNs. This protocol provides more security using the digital signature crypto system that is based on the RSA algorithm and MD5 hash function. In this protocol, they assume that deployment of nodes is random, and wireless sensor network is like a undirected graph. Each sensor node has fixed transmission range. Also, each sensor node has private and public keys. The EENDMRP protocol operates in two phases: first is route construction phase and second is the data transmission phase. In route construction phase, every node creates a routing table. Each sensor node transmits once the packet in route construction and also maintains its own routing table. In data transmission phase, the primary path is selected from source to destination based on the maximum path cost. In order to choose the maximum path cost they also consider the remaining energy of a node and queue length. The results show the improved data packet delivery, reduced average end-to-end delay, normalized routing load and less energy consumption.

2.8. Secure and Energy Aware Routing Protocol (SEAR)

Tang *et al*. [8] have proposed a secure and energy aware routing (SEAR) protocol. In this protocol, they addressed the two key issues: energy consumption and source location privacy. The proposed algorithm used the energy balance control and security intensity parameters. The energy balance control is used to maintain energy balance and also used to improve the lifetime of a network. The routing security is provided by security level that is used to examine the probabilistic allocation of a random walking. The security level defines the message source on a message level or system level. They assume that sensor nodes are deployed randomly, have partial and non-replenishable energy resource. A multi-hop routing strategy is used to forward the packet to the sink node. Every sensor node has a node ID related to the location where encrypted message is created. Every sensor node has the knowledge of its location in the sensor area and also instant adjacent grids and their energy level. The SEAR algorithm provides two methods for packet forwarding: one is shortest path forwarding on the bases of geographical information, and second is random forwarding, which is used for source privacy and jamming avoidance. The advantages of using the this protocol are: it consumes less energy which increases the network life; the routing path is selected dynamically by using geographical information and residual energy in neighboring grids; it also provides security against the threats in a sensor network. The results show that it consumes less energy, and maximize the probability of data packet delivery.

2.9. Secure Energy efficient Load Balancing Multipath Routing Protocol (TSEL)

Yuvaraju and Rani [9] have presented the TSEL (Secure Energy Efficient Load Balancing Multipath Routing Protocol with Transmission Power Adjustment). It is a multipath routing protocol, which utilizes the energy efficiently. It ensures message authentication and integrity by using a digital signature. It uses MD5 hash function and RSA public key algorithm. Each sensor node has its own private and public key. It constructs the route, which is based on the criteria constitute of ten steps. After the construction of a route, it selects the primary path from source to destination based on disjoint node multipath. The cost of the selected path is calculated based on remaining energy and the queue length of node i.e. $NC=RE*FQL$. The results of this protocol show that it increases the lifetime of the sensor network and it also consumes less energy.

2.10. Efficient and Secure Routing Protocols through SNR based Dynamic Clustering (ESRPSDC)

Ganesh and Amutha [10] have proposed an efficient and secure routing protocol for wireless sensor networks through signal to noise ratio (SNR) based dynamic clustering (ESRPSDC). This process is divided into five phases: initialization, energy based cluster head (CH) selection, signal to noise ratio (SNR) based Cluster Head selection by Non-Cluster Head (NCH) nodes, data forwarding using inter cluster routing, and identification of the intruder. In Initialization phase, the base station broadcast the request messages to the whole network. Nodes are divided equally into the clusters then nodes formed the cluster ID and cluster table. In the energy based cluster head (CH) selection phase, it checks each node's energy level. Any node whose energy level is greater than the threshold value will be considered for the cluster head selection. If it is not greater, then it elects the NCH node. NCH nodes will select their cluster head based on SNR. Data forwarding is done through inter-cluster routing mechanism, which consumes less energy. When all data is received from the cluster members, cluster heads performs the data aggregation function and then forwards it to the base station. Intrusion is identified by analyzing the routing pattern. Authors assumed that all sensor nodes in the network are heterogeneous and have limited resources. Every node forwards its information to the CH. The base station is located distance away from the sensor nodes and it is static. Transmission power level is fixed. Each node in a sensor network is not equipped with GPS unit. The results show that packet delivery ratio (PDR) is increased and end-to-end delay and power consumption is reduced.

2.11. Efficient and Secure Routing Protocol using Mine Detection (ESRP-M)

Subramanian and Amutha [11] have proposed an efficient and secure routing protocol for wireless sensor networks using Mine detection (ESRP-M). In this paper, they modified the triple umpiring system (TUS). The TUS has shown its enhanced performance on MANET in which every node in a path from source to destination has two roles to carry out: one is packet forwarding and second is umpiring. They have proposed the mine detection model in the TUS. The behavior of an attack is measured actively and passively. They send the packets that contain dummy information for detection of mines and introducers. The Mine detection system grants a complementary means of protection to wireless sensor network. They assume that nodes are deployed randomly. Also, nodes have the mine detection algorithm and a clock, which is loosely synchronized. A compromised node or implanted node can inject false information in the network. The simulation results show that end-to-end delay is reduced and packet delivery ratio (PDR) is increased.

2.12. Cost-aware SEcure Routing Protocol (CASER)

Tang *et al.* [12] have purposed a cost-aware secure routing (CASER) protocol for wireless sensor networks. They described that cost-aware based routing techniques can be applied to addressing the message delivery requirements. They find out that energy consumption is relentlessly disproportional to a uniform energy deployment for a particular network topology, which decreases the duration of a sensor networks. To overcome this problem, they chose the non-uniform energy deployment strategy. The advantages of using this protocol are: it consumes less energy and increase network lifetime, and it also uses the multiple routing approaches on the base of routing needs. They also described a model that contain sensor nodes and sink node which have limited energy resources. For security, each node has unique identities. Authors also assume that adversaries have enough energy resources, sufficient computational capacity and adequate memory for data storage space. Also they can perform attacks like flooding, but they are not capable of examining the whole network. The results show that message delivery ratio is increased, and end-to-end delay is reduced.

2.13. A Secure Cluster based Multipath Routing Protocol (SCMRP)

Kumar *et al*. [13] have proposed a secure cluster based multipath routing protocol (SCMRP). It provides both end to end and point-to-point security. Through multipath routing protocol, flexibility can be improved. The SCMRP is a proactive that computes all routes prior. This routing protocol is divided into five different phases: i) neighbor detection and topology construction phase, ii) cluster formation phase, iii) re-clustering and re-routing phase, iv) pair wise key distribution phase, and v) data transmission phase. These phases are useful in diminishing traffic on a network and accumulate energy. The neighbor information is encrypted using shared key and integrity of base station confirmed using MAC. The SCMRP provides protection against various attacks like selective forwarding, sybil, spoofing. The base station (BS) gather a list of all neighboring sensor nodes and then find the multiple paths by applying the depth first search (DFS) algorithm. They assumed that initially sensor nodes will be deployed randomly. They assumed a homogeneous system with nodes have similar features like computing and storage. The base station is secure, and each node has unique ID. There will be one hope communication among cluster node and cluster head**.**

2.14. A Hybrid Secure Node Joining (HySecNJoining) Algorithm

Kalita and Kar [14] have presented the hybrid secure node-joining (HySecNJoining) algorithm. To join the new node successfully, the proposed algorithm is based on both asymmetric and symmetric key cryptography. There are three different types of keys used in this algorithm. First is Hook key that is used for joining the new node in wireless sensor network. Second is one hop key that is a symmetric key. It used for both base station authorization and neighbor node communication. Third is K_A^{pri}/K_A^{pub} asymmetric key for each sensor node. Messages are encrypted and decrypted using this key. This algorithm operates in two phases: first is neighbor phase, in which each new node is authenticated by the one hope key. For this purpose, they swap their public keys for communication between nodes. Second phase is authentication by base station phase, in which each node sends its request to the base station. If the joining request is successful then it forwards the public key of a base station to the node. Base station uses the one hope key for encryption and it uses the private key for authentication. They also assume that digital signature has not any public key, both one-hope key and hook key is used for validation of public key of the sensor node. Forwarding node has the subset of all public keys of sensor nodes. During the process of sending and receiving messages, each node validates the message using the public key.

3. Attacks and Security Approaches

Existing secure routing protocols uses various symmetric and asymmetric cryptographic approaches to provide protection against various attacks like, eavesdropping, DoS attack, Sybil attack, spoofing, jamming etc. Table 1 summarizes the details about the secure routing protocols provide protection against which types of attacks.

Table 1. Attacks on OS Layer and Security Different Approaches against These Attacks

Secure Routing Protocols	**Attack on Layer**	**Type of Attacks**	**Security Approach**
LS-LEACH [1]	Link layer	Eavesdropping	Symmetric Key Cryptography
SCRA [4]	Network layer	Dos attack	Symmetric Key Cryptography
Secure Directed Diffusion [5]	Network layer	Selective forwarding	Hybrid
TEESR [6]	Data link layer	Sybil attack	Symmetric Key Cryptography
EENDMRP [7]	Network layer	Spoofing, altering, Altered Routing	Asymmetric Key Cryptography
SEAR [8]	Physical layer	Jamming, Routing Traceback	Symmetric Key Cryptography
tSEL [9]	Network layer	Altered Routing, Byzantine	Asymmetric Key Cryptography
CASER [12]	Physical and Link layer	Routing traceback Jamming, Eavesdropping	Symmetric Key Cryptography
SCMRP [13]	Network Layer	Sinkhole, Wormhole, Selective forwarding	Asymmetric Key Cryptography
HySecNJog [14]	Transport layer	Hello Flood attack	Hybrid

4. Taxonomy of Secure Routing Protocols

We divided the secure routing protocols into two different categories one is a cluster base and second is none cluster based figure 1. In the cluster bases routing, a network is divided into sub structures we call it cluster, for the coordination of sub-structure every node in network have its own cluster head. It is also used to transfer data among the nodes in the network. In none cluster base approaches there is no cluster in the network they use approaches other than this approach. Then we further subdivided these two categories into three subcategories. One is symmetric key cryptography second is asymmetric key cryptography and third is hybrid. In symmetric key cryptography it encrypt the message using same key also use the same key for decryption of the message. In asymmetric key cryptography, it encrypts the message using same key also use the same key for decryption of the message. In asymmetric key cryptography, two different keys are used. One is public key other is private key. In hybrid, both asymmetric and symmetric cryptography approaches are used.

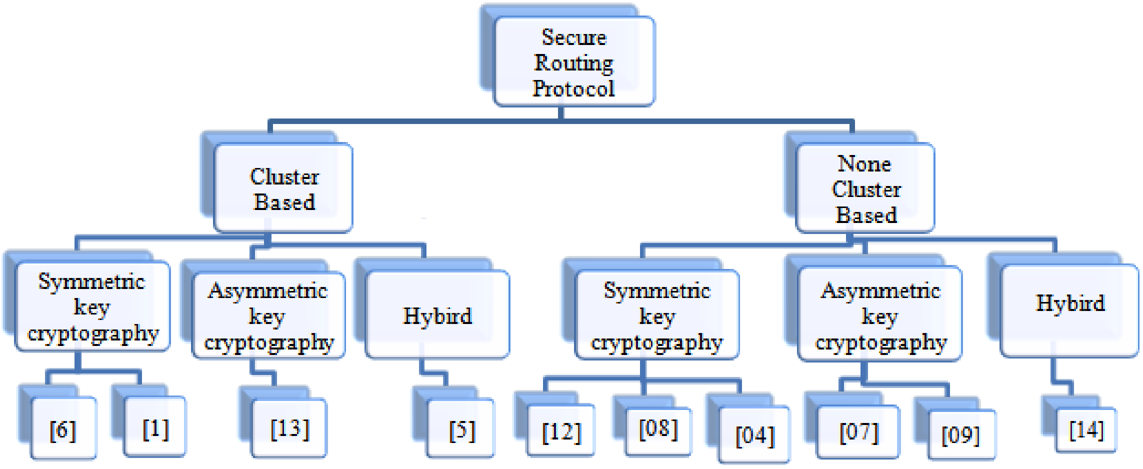
Secure Routing Protocol
Cluster Based
None Cluster Based
Symmetric key cryptography
Asymmetric key cryptography
Hybird
Symmetric key cryptography
Asymmetric key cryptography
Hybird
[6]
[1]
[13]
[5]
[12]
[08]
[04]
[07]
[09]
[14]

Fig.1. Taxonomy of Secure Routing Protocols

5. Comparison of Secure Routing Protocols

Table 2 provides a qualitative comparison of the existing secure routing protocols of WSNs. For this purpose, we have used the following parameters: 1) protocol type, 2) protocol classification, 3) security assumption, and 4) environmental assumptions

According to this table, Lata *et al.* [6], and Alshowkan *et al.* [1] have adopted the cluster based symmetric key cryptography approach for the security of routing protocols. Whereas, Tang *et al.* [12], Tingting *et al.* [8], and Khan [4] have adopted none cluster based symmetric key cryptography approach. Kumar et al. [13] have adopted the cluster based asymmetric cryptography approach, whereas D'Souza *et al.* [7], Yuvaraju and K. Rani *et al.* [9] have adopted the none cluster-based asymmetric cryptographic approach. To overcome the drawbacks of symmetric and asymmetric cryptographic approaches, Belkadi *et al.* [5], and Kalita *et al.* [14] have adopted the hybrid approach to secure the routing protocol. This comparison gives us the clear idea of different approaches for secure routing protocols and how to deal with these security issues using appropriate approach, which is efficient, secure, easy to use and less costly.

Table 2. Comparison of Secure Routing Protocols

Routing Protocols	**Protocol type**	**Protocol classification**	**Security Assumptions**	**Environmental Assumptions**
LS-LEACH [1]	Cluster Based	Hierarchal	There are two keys needed private key and group key; private key is shared with base station and group key is used to join the clusters.	No. of cluster heads should not be greater than the 5% of total nodes.
SCRA [4]	None Cluster Based		Secret keys for sensor motes (SMs), pair-wise keys for broadcast authentication (BA), SMs and cluster head (CHs).	SMs will be distinct, inactive, outfitted with resistant hardware and compute space by signal-strength.
Secure Directed Diffusion [5]	Cluster Based	Data Centric	3 keys, IKu, Kpair, BK are used for providing secure communication. Individual key (IKu) is used between a node and a base station; Pair-wise key (Kpair) is used among node and its neighbors; Global key (BK) is distributed by base station with all nodes; MAC is used for data integrity and authentication; RC5 algorithm is used for confidently.	They assume energy as a major constraint, increase network lifetime and allow unicast, broadcast that flexible in term of energy consumption.
TEESR [6]	Cluster Based	Hierarchal	MAC integrity of message, Symmetric key for discovering a safe route against attacks, Cluster Heads uses the Pair key.	They assume that this protocol limits malicious node in its neighbor using the suitable authentication and flooding method. It will perform the resource intensive reckoning.
EENDMRP [7]	None Cluster Based	QoS	2 keys; each node have private and public Key and Common Hash function all nodes in the network.	Random node deployment; fixed transmission range for sensor nodes; and WSN is like an undirected graph.
SEAR [8]	None Cluster Based	Location Based	Massage is encrypted using the shared secret key among the node/grid and sink node.	SN randomly deployed; Partial and non-replenishable energy resource; Node ID used for location information; SN have location, adjacent grid and energy information.
tSEL [9]	None Cluster Based	Multipath	Each node has its own private and public key. RSA public key and MD5 hash algorithm for security.	Primary path is selected and data load is distributed between multiple paths. It has more loads as compared to other path. Nodes have flexible transmission power.
CASER [12]	None Cluster Based	Multipath	A key is shared with each node and message is encrypted using this key.	SNs randomly deployed; adversaries have energy resources, ample computational capacity, adequate memory and can attack like flooding, but not capable to examine the whole network.
SCMRP [13]	Cluster Based	Hierarchal	Each node has unique ID and a certificate for authentication and also unique key and public key for base station for communication. Paired key (private and public key) is used to encrypt the message and also decrypted the message.	SNs deployed randomly; all nodes are homogeneous, base station is secure there will be one hope communication among cluster node and cluster head.
HySecNJoining [14]	None Cluster Based	Hybrid	3 keys are used: 1) Hook key, 2) Hop key, 3) K_A^{pri} /K_A^{pub} (asymmetric key) Hook Key is used to join a new node. Base station and neighboring nodes both use Hop key for communication and authorization. K_A^{pri} /K_A^{pub} (asymmetric key pair) is used for encryption and decryption.	In the neighbour authentication approach will avoid unnecessary packets moving in the network, For communication there will no session key, any node can authenticate the message using the public key which is in the store.

6. Future Challenges and Issues

With the advancement in wireless sensor network technology, its usage in our daily life is increasing. Even though there is a lot of work has been done for the secure transmission, but the issues regarding security of WSNs still not overcome yet.

- From the literature survey, we found that most of the existing routing protocols are not providing basic security features like confidently, authentication integrity, and reliability.
- A challenging issue in designing a secure routing protocol for a wireless sensor network is availability of limited resources of sensor node e.g., storage, and computation power. In wireless sensor network, energy efficiency is also an important issue
- Another main problem is that there is no security evaluation on framework for the routing protocols in WSNs that is needed for the comparison purpose. Currently, every researcher uses their own criteria for evaluation.
- Furthermore, most of the existing schemes ignore the issues of accountability and freshness of data.
- Use of traditional symmetric and asymmetric approaches is computationally expensive task for the sensor nodes. It will be interesting to see the effects of elliptic curve cryptography in secure routing protocols.

7. Conclusions

Wireless sensor network comprises of resource constraint sensor nodes. That is why, designing and selecting an appropriate secure routing protocol for the network is a tough task. In this research paper, firstly, we have discussed the various types of security attacks. Secondly, we have presented a taxonomy of secure routing protocol and then provided a qualitative comparison. Finally, we have highlighted future challenging issues. Results show that most of the existing routing schemes are not very efficient in providing security.

References

[1] M. Alshowkan, K. Elleithy, and H. Alhassan, “Ls-leach: A new secure and energy efficient routing protocol for wireless sensor networks,” 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Oct 2013, pp. 215–220.

[2] B. Lata, V. Tejaswi, K. Shaila, M. Raghavendra, K. Venugopal, S. Iyengar, and L. Patnaik, “SGR: Secure geographical routing in wireless sensor networks,” 9th International Conference on Industrial and Information Systems (ICIIS), Dec 2014, pp. 1 – 6.

[3] H. Cheng, C. Rong, and G. Yang, “Design and analysis of a secure routing protocol algorithm for wireless sensor networks,” IEEE International Conference on Advanced Information Networking and Applications (AINA), March 2011, pp. 475–480.

[4] F. Khan, “Secure communication and routing architecture in wireless sensor networks,” 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE), Oct 2014, pp. 647–650.

[5] M. BELKADI, R. AOUDJIT, M. DAOUI, and M. LALAM, “Energy efficient secure directed diffusion protocol for wireless sensor networks,” International Journal of Information Technology and Computer Science (IJITCS), vol. 6, no. 1, p. 50, 2013.

[6] N. Durrani, N. Kafi, J. Shamsi, W. Haider, and A. Abbsi, “Secure multi-hop routing protocols in wireless sensor networks: Requirements, challenges and solutions,” 2013 Eighth International Conference on Digital Information Management (ICDIM), , Sept 2013, pp. 41–48.

[7] S. G, R. D’Souza, and G. Varaprasad, “Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks,” Sensors Journal, IEEE, vol. 12, no. 10, pp. 2941–2949, Oct 2012.

[8] D. Tang, T. Jiang, and J. Ren, “Secure and energy aware routing (sear) in wireless sensor networks,” in Global Telecommunications Conference (GLOBECOM 2010), IEEE, Dec 2010, pp. 1 – 5.

[9] M. Yuvaraju and K. Rani, “Secure energy efficient load balancing multipath routing protocol with power management for wireless sensor networks,” 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), July 2014, pp. 331–335.

[10] S. Ganesh and R. Amutha, “Efficient and secure routing protocol for wireless sensor networks through snr based dynamic clustering mechanisms,” Journal of Communications and Networks, vol. 15, no. 4 , pp. 422–429, Aug 2013.

[11] G. Subramanian and R. Amutha, “Efficient and secure routing protocol for wireless sensor networks using mine detection an extension of triple umpiring system for WSN,” 2012 8th International Conference on Computing Technology and Information Management (ICCM), vol. 1 , April 2012, pp. 141–145.

[12] D. Tang, T. Li, J. Ren, and J. Wu, “Cost-aware secure routing (CASER) protocol design for wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 960–973, April 2015.

[13] S. Kumar and S. Jena, “Scmrp: Secure cluster based multipath routing protocol for wireless sensor networks,” 2010 Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), Dec 2010, pp. 1 – 6.

[14] H. Kalita and A. Kar, “HySecNJoining: A hybrid secure node joining algorithm for wireless sensor network,” 2011 Third International Conference on Communication Systems and Networks (COMSNETS), Jan 2011, pp. 1-6.

[15] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad, "The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures", IJWMT, vol.2, no.2, pp.33-44, 2012.

Authors’ Profiles

Yasir Arfat is currently a M.S. student at King Abdulaziz University, Jeddah, Saudi Arabia. He received his BS (SE) degree in Software Engineering with Distinction from University of Azad, Jammu &Kashmir, Pakistan in 2011. His research interests include network security, software security, software agent systems and exascale systems.

Riaz Ahmed Shaikh is an Assistant Professor at the CS Dept. in the King Abdulaziz University, Jeddah, Saudi Arabia. He obtained his Ph.D. from Computer Engineering Dept., of Kyung Hee University, Korea, 2009, and M.S. in IT from the National University of Sciences and Technology, Pakistan, 2005. His research interest includes privacy, security, trust management, wireless sensor network.

How to cite this paper: Yasir Arfat, Riaz Ahmed Shaikh,"A Survey on Secure Routing Protocols in Wireless Sensor Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.6, No.3, pp.9-19, 2016.DOI: 10.5815/ijwmt.2016.03.02