Security in Wireless Sensor Network: Approaches and Issues

Raja Waseem Anwar[1], Majid Bakhtiari[2], Anazida Zainal[3], Kashif Naseer Qureshi[4]
Department of Communication, Faculty of Computing,
Universiti Teknologi Malaysia, Skudai, 81310, Johor Darul Takzim, Malaysia
*Corresponding author, e-mail: rajawaseem@gmail.com[1], bakhtiari@utm.my[2], anazida@utm.my[3], kashifnq@gmail.com[4]

Abstract

Wireless sensor network is a tremendous emerging technology provides communication services for environmental monitoring and target tracking for mass public and military. With increasing of this smart network popularity sensor network faced various challenges and threats. The inclusion of wireless sensor nodes also incurs different types of security threats in network. Mostly networks are using shared key approaches to make less communication overhead, but still network compromise with replay impersonation and compromise attacks. The existing proposed schemes are not fully addressed other network resources such as energy and speed, etc. The intent of this paper is to provide a comprehensive security requirement, detail about security attacks in network and discuss the existing security schemes.

Keywords*: security, attacks, cryptography, wormhole, denial of services*

1. Introduction

Wireless sensor networks is an emerging technology comprise with disperse small tiny sensor nodes for sensing the environment for specific purpose. These tiny sensor devices communicate with each other in specific geographic area for target tracking, environmental monitoring and surveillance [1]. Recently, the WSNs bring significant advantages compared to traditional communication technologies in every field of life for sense and monitor such as healthcare, homeland security, transportation and military operations, etc. [2, 3]. In some applications the data is more critical and security mechanisms are essential to ensure confidentiality, authenticity and integrity. In wireless sensor networks the sensor nodes are densely deployed and perform signal processing, computation to achieve robust and scalable networks. The communication among the sensors is possible through wireless sensor transceivers. These sensor nodes are combined with 8-bit processor with memory and with small capacity of storing the data. Further these sensors gather the data and send to sink node for further processing. However, complex and harsh environment pose great challenges to ensure the reliability of WSN communication. Basically the main challenge for employing and security scheme is created through the sensors size, processing power, memory and type of task. To overcome these security issues different techniques have been implemented such as cryptography, steganography, etc.

In this paper, we discuss the security challenges and issues for wireless sensor networks and explore some decisive parameters that need widespread investigations.

2. Security Requirements

The wireless sensor network has unique characteristics and need some security requirements. The message authentication is important and required for many applications in sensor network for administrative responsibilities such as network controlling and reprogramming sensor node duty cycle. In network, the adversary simply inject messages and receiver need to make confident that data used for decision making process creates from source [4]. The data authentication avoids illegal parties from participating in the network along with genuine sensor nodes should be capable to detect messages from unauthorized nodes. The second security requirement is integrity, where data integrity sure that the received data is

Received Apr 26, 2014; Revised July 26, 2015; Accepted August 10, 2015

not effected and transit to attacker. Data confidentiality refers to hide the data from unauthorized parties. Normally for data confidentiality encryption the data with secret key is used for secure network. The encryption techniques are more costly and strict limitations in wireless sensor network. These techniques consume additional energy and computational resources in network. If data integrity and confidentiality are assured, the sensor network need freshness of each message. The data freshness refer to ensure that data is recent and not replayed old messages through timestamp added in packet.

3. Security Threats in Wireless Sensor Networks

In wireless sensor networks, broadly the security attacks are categorized into two levels: attacks against security mechanism and attacks against routing mechanism. In this section, we discuss these stacks in detail.

The first attack is denial of service [5, 6], refer to unintentional failure of nodes and exhaust the available resources through sending extra packets to legitimate the network. These attacks are serious and critical threat for network and not only subvert, destroy and disrupt the network, also for any event that diminishes a network capability. There are different types of DoS attacks performed in wireless sensor network in different layers. The physical layer attacks could be tampering and jamming the network and data link layer attacks collide and exhaust the network. The network level attacks are performed for greed, neglect, misdirection and used for black holing. The attacks related with transport layer are used for desynchronization and malicious flooding. For prevent from these attacks, wireless network adopted strong authentication and identification mechanism on payments.

Some attacks are related on information in transit, where sensors monitor changes of specific parameters and report to sink according to the requirement [7]. During sending the report the transmitted information is altered or spoofed. After the vulnerable network, any attacker could be monitor the traffic flow, intercept and interrupt the data packets and insert wrong information toward the sink node. Due to limited communication range and other resources of sensors, attacker always attack with high processing power and communication range for data modification in network.

Sybil attack is another attack in wireless sensor network, where these attacks degrade the integrity of data, security and resource utilization. In many scenarios the sensors nodes work together and use distribution of subtasks and redundancy of information. In these scenarios, the single sensor node show the multiple identities in network and reduce effectiveness of distributed resources, multipath routing, dispersity and topology maintenance [8]. Most of the wireless ad hoc networks have been suffered from these attacks. To prevent from these attacks, researchers have been proposed different routing strategies, which are discussed in coming section.

Another types are blackhole and sinkhole attacks [9], where a malicious node attract the traffic in network. This type is common in flooding based protocols, where attacker listen the request for routes and replies to target nodes and contains the high quality or shortest path to the base station. Whenever the malicious node is able to communicate and do anything in network with other nodes, the whole network is affected. The hello flood attack uses hello or beacon messages as a weapon to convince the sensor nodes in network [10]. In these attacks the high transmission range is used with high processing powers in large area of sensor networks. The sensor nodes are convinced about adversary in neighbors. Whenever the the sending information forward to base station the victim node try to go through from attacker and spoofed by the attacker.

One of the critical attack in wireless sensor network is wormhole attack [11]. In this type of attack the attacker record the packets and tunnel to another location. The tunneling and retransmitting of bits is a threating act because these attacks are performed at initial neighbor discovering stage. The below Table 1 shows some popular attacks, level and their defensive mechanism in wireless network.

Table 1. Attacks level and their defensive mechanism

S/No	Attack	Level	Defense mechanism
1	Denial of Services (Dos)	Physical	Encryption, Tamper Proofing, Priority Messages Hiding
2	Tampering	Physical	Hiding, Encryption
3	Jamming	MAC Layer Level	Error Correcting
4	Collision	MAC Layer Level	Codes
5	Sybil	Network	Identity certificates
6	Wormhole	Network	Probing, Redundancy, Authorization
7	Sink Hole	Network	Monitoring
8	Flooding	Network	Monitoring
9	Desynchronization	Application	Aggregate commit framework
10	Aggregation	Application	Aggregate commit framework

4. Feasible Security Schemes for Wireless Sensor Networks

The term security is refer to encompassing the features of integrity, authentication, privacy and nonrepudiation, etc. Recently, the usage of wireless sensors in different applications increase the risk of secure transmission over the network. To protect and secure the network from different attacks in network, various types of approaches have been countered [12]. In this section, we discuss these approaches in details.

The first approach is cryptography, where encryption and decryption approaches formulated for traditional wired networks. These approaches are less suitable to implement in wireless and particularly in wireless sensor scenarios. The wireless sensor networks are consist with small size sensors with low battery power, less memory and processing capabilities [13, 14]. Encryption schemes need extra bits, transmission, memory and processing power. These are significant resources for sensor longevity. Encryption schemes also suffered from packet loss, jitter in wireless sensor networks. Further, the implementation of encryption schemes in wireless sensor network arise various questions such as how the key are assigned, managed and revoked, etc. Because sensor networks are unattended scenarios. There are different techniques of key management have been proposed for providing the security mechanism by confidentiality, authentication and integrity for secure the network. These techniques have many advantages and disadvantages such as shared key take minimum resources but disadvantage is single node reveal the secret key and allow decryption of all network traffic [15]. The public key cryptography is used for data encryption and beyond computation resources of sensor node. It is used only in the process of key distribution in WSNs. Another bootstrapping key is for trusted base station, where the single key share with other nodes through base station. The main disadvantage of this key is failure of base station because it is single point for sharing the key. The key pre-distribution approach is used when the key information is implanted in sensor node before deployment [16]. This is same like shared key, where capture one node lead to compromise whole network. There is another key-redistribution protocol developed used random set of keys assign to sensor node [8]. Every sensor node compute or discover the common key with neighbors. These all authentication keys are used for secure the communication in network.

Another term steganography is refer to hiding the existence of message while cryptography hiding the content of message [17]. This is a practice for concealing message and convert communication through embedding a message into image, sound and video, etc. Steganography is used to hide the existence of covert channel and useful in sending the secret data publically without sender information. Mostly this approach is applied in digital images by changing the least bit and not easy detected with human eye. This approach is feasible for redundant and error-tolerant communication. However, the wireless sensor networks security is not directly related to steganography and processing the video and audio data with insufficient resources.

Physical layer secure access is refer to provide security through frequency hopping in network. This is based on dynamic combination of parameters such as hopping set, time interval and sequence patterns with less processing, memory and energy consumption. The significant point in secure access is efficient design for hopping order modified in less time compared to required time for discovering, for employing source and destination must synchronize with each other.

Wireless sensor networks security is in top priority worldwide for researchers and development sectors. The sensor network has limited resources in terms of node size, density, unknown topology and high risk of security attacks to unattended sensors. In this section we discuss the proposed security solutions for wireless sensor network.

Wireless sensor network has limited resources, unattended environment with unstable channel conditions. The designing of reliable and stable routing protocols always a challenge to improve the network efficiency.

Most of the security solutions are based on single-path routing, where source node choose a single path toward the base station or sink node without satisfactory consideration of traffic load, reliability and energy. In single path solutions the route discovery can be performed with less computational complexity and resource utilization. The limited capacity of single path highly decreases achievable network throughput [18, 19].

Geographical routing protocols with location information for sensor node are valuable example for wireless senor network. The geographical information is used for estimate the transmitted packets delay such as stateless protocol for end-to-end delay (SPEED) [20]. The location information is determine through self-configuring localization and global positioning systems [21]. These solutions are reliable because of their low overhead and minimum state stored to forward data and flexible with topological changes. Further, these solutions save bandwidth and energy due to discovering floods are not needed. The greedy approaches also have been proposed for reliable links, where unreliable neighbors bypass during transmission and only highest value of packet reception rate multiplied through distance [22, 23]. These approaches are not feasible for real time applications because in each step of packet forwarding sensors need to evaluate different metrics. These metrics increase the computation time and end-to-end delay in network. The greedy approaches have another drawback is that the transmission may fail in the presence of optimal path between source and sink node especially in nosy environments. The proactive routing is another example for reliability. The DTRP [24] was proposed to provide reliability through multi-path redundancy and scalability. The approach is able to broadcast data packets to the air and reduce complexity of data link layer. On the other hand these approaches are using more energy.

The multilayer approaches are proposed to provide security in layers of protocols stack [25]. The one of the main disadvantage of these approaches is redundant security provisioning in network. The redundant is refer to many protocol layers within the network stack capable for providing security services to the same attack. It is a no adaptive security service in terms of counterattacks approach in some protocol layer without guarantee security all the times. In addition, the power inefficiency is not be addressed at any single layer in network stack.

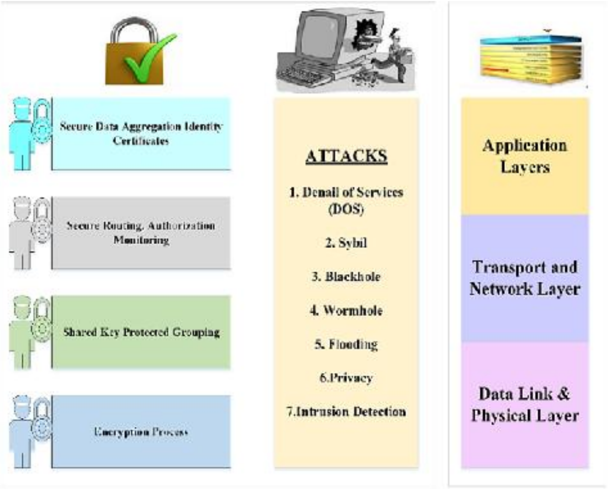
Secure Data Aggregation Identity Certificates
Secure Routing, Authorization Monitoring
Shared Key Protected Grouping
Encryption Process
ATTACKS
1. Denail of Services (DOS)
2. Sybil
3. Blackhole
4. Wormhole
5. Flooding
6.Privacy
7.Intrusion Detection
Application Layers
Transport and Network Layer
Data Link & Physical Layer

Figure 1. Security in different levels

The wireless sensor network has its unique and different features such as small in size, power constraints, etc. Key management area has been gain a wide attention in wireless sensor area. The key establishment is done by various public key protocols. In this process the network is safe from outside attacks through apply key infrastructure. These schemes are not so efficient because of non-resilience and not scalable. The wireless network composed with many tiny size sensor nodes and automated devices. These sensors bind themselves for specific task in environment such as monitoring. The group members communicate with each other and try to establishes secure operations. However, this secure grouping mechanism is not intensive [26]. The encryption is another scheme for wireless network but these schemes insignificant due to sensor node to eavesdrop or even add messages in network [27]. To address these issues the different solutions have been proposed in shape of message authentication codes, encryption approaches and symmetric and public keys.

Data aggregation schemes are used for defenseless networks against the denial of services attacks. The data transferring is one of the significant trouble due to network overhead and traffic. To address this problem the sensor node aggregates measurements toward the sink node before sending the data. An adversary node can select or produce false report and affecting the credibility of data. To solve these issues resilient functions are used to discover and report about forged reports by authenticity of data [27].

There are many types of security protocols have been proposed to build a secure and reliable network communication. These SPINS (security protocols for sensor network) build a blocks and optimized the resources. These schemes offered many security properties in network such as semantic security, data freshness, authentication, protection and low communication overhead. Another lightweight package is TinySec included in sensor nodes. This package provide authenticated encryption and only authentication [28]. The below Table 2 shows some proposed schemes for wireless sensor network.

Table 3. Security schemes for wireless sensor network

S/No	Security Scheme	Attack Deterred	Description
1	Wormhole based [29]	DoS (Jamming)	This scheme use wormhole to avoid jamming in network.
2	TIK [11]	Wormhole and data spoofing	This scheme is based on symmetric cryptography and need accurate time synchronization for all parties in network.
3	TinySec [30]	Message replay attack and data spoofing	This scheme is for providing the data authenticity, integrity and confidentiality in network.
4	REWARD [31]	Blackhole Attack	In this scheme the neighbor transmission is watching for detection.
5	Random Key Predistribution [32, 33]	Data spoofing, Attack on transit information	It is protect the network even though some part of network effected and also provide authentication.
6	In band Wormhole [34]	DoS (Jaming)	In this scheme an adversary make a link between two regions by colluding network.
7	Nature Based Trust Security [35]	Grayhole attack	In this scheme the trust value is calculated to prevent from grayhole attack.

5. Conclusion

Most of the security schemes in wireless sensor network are used to protect the network from internal and external security attacks. To prevent from different attacks the network need an efficient detection mechanism to ensure the holistic security in wireless sensor network. Many different types of security approaches have been proposed for different levels and based on network specific models. Still network need a combine effort or a common model to ensure the security in network. There is a need to combine all the level security in collaborative manner and still this phenomena is challenge for researchers. Wireless sensor network has its own limitations and special features especially limited computational power and energy. The future security scheme will be efficient in terms of cost and energy. This review will help the researchers for design and prevent network from different attacks.

References

[1] RW Anwar, M Bakhtiari, A Zainal, AH Abdullah, KN Qureshi. Security issues and attacks in wireless sensor network. *World Applied Sciences Journal.* 2014; 30: 1224-1227.

[2] KN Qureshi, AH Abdullah, G Ullah. *Sensor based Vehicle Environment Perception Information System.* In 4 IEEE International Conference on Ubiquitous Intelligence and Computing/International Conference on Autonomic and Trusted Computing/International Conference on Scalable Computing and Communications and Its Associated Workshops. 2014: 697-700.

[3] KN Qureshi, AH Abdullah. Wireless Sensor Based Hybrid Architecture for Vehicular Ad hoc Networks. *TELKOMNIKA Telecommunication*, Computing, Electronics and Control. 2014; 12.

[4] VC Giruka, M Singhal, J Royalty, S Varanasi. Security in wireless sensor networks. *Wireless communications and mobile computing.* 2008; 8: 1.

[5] BT Wang, H Schulzrinne. *An IP traceback mechanism for reflective DoS attacks.* In Electrical and Computer Engineering, 2004. Canada. 2004: 901-904.

[6] V Durcekova, L Schwartz, N Shahmehri. *Sophisticated denial of service attacks aimed at application layer*. in ELEKTRO, 2012. 2012: 55-60.

[7] PP Charles, P Shari. Security in computing. Prentice-Hall, lnc. 2008.

[8] J Newsome, E Shi, D Song, A Perrig. *The sybil attack in sensor networks: analysis & defenses*. In Proceedings of the 3rd international symposium on Information processing in sensor networks. 2004: 259-268.

[9] BJ Culpepper, HC Tseng. *Sinkhole intrusion indicators in DSR MANETs.* In Broadband Networks, 2004, BroadNets 2004 Proceedings, First International Conference. 2004: 681-688.

[10] C Karlof, D Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks.* 2003; 1: 293-315.

[11] YC Hu, A Perrig, DB Johnson. *Packet leashes: a defense against wormhole attacks in wireless networks.* In INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies. 2003: 1976-1986.

[12] RW Anwar, M Bakhtiari, A Zainal, KN Qureshi. Malicious Node Detection Through Trust Aware Routing in Wireless Sensor Networks. *Journal of Theoretical and Applied Information Technology*. 2015; 74.

[13] G Anastasi, M Conti, M Di Francesco, A Passarella. Energy conservation in wireless sensor networks: A survey. *Ad hoc networks*. 2009; 7: 537-568.

[14] V Potdar, A Sharif, E Chang. *Wireless sensor networks: A survey.* In Advanced Information Networking and Applications Workshops, WAINA’09, International Conference. 2009: 636-641.

[15] A Perrig, J Stankovic, D Wagner. Security in wireless sensor networks. *Communications of the ACM.* 2004; 47: 53-57.

[16] W Du, J Deng, YS Han, S Chen, PK Varshney. *A key management scheme for wireless sensor networks using deployment knowledge.* In INFOCOM 2004, Twenty-third Annual Joint conference of the IEEE computer and communications societies. 2004.

[17] I Cox, M Miller, J Bloom, J Fridrich, T Kalker. Digital watermarking and steganography. Morgan Kaufmann. 2007.

[18] JN Al-Karaki, AE Kamal. *Routing techniques in wireless sensor networks: a survey.* Wireless communications, IEEE. 2004; 11: 6-28.

[19] K Akkaya, M Younis. A survey on routing protocols for wireless sensor networks. *Ad hoc networks.* 2005; 3: 325-349.

[20] S Fekete, A Kroller, D Pfisterer, S Fischer, C Buschmann. *Locating and bypassing routing holes in sensor networks.* In Proceedings of International Workshop on Algorithmic Aspects of Wireless Sensor Networks. 2004.

[21] KN Qureshi, AH Abdullah. Localization-Based System Challenges in Vehicular Ad Hoc Networks: Survey. *Smart Computing Review*. 2014; 4: 515-528.

[22] G Egeland, PE Engelstad. *The availability and reliability of wireless multi-hop networks with stochastic link failures.* Selected Areas in Communications, IEEE Journal. 2009; 27: 1132-1146.

[23] Y Xu, WC Lee. *Exploring spatial correlation for link quality estimation in wireless sensor networks*. In Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International Conference. 2006; 10: 211.

[24] MS Nassr, J Jun, SJ Eidenbenz, A Hansson, AM Mielke. *Scalable and reliable sensor network routing: Performance study from field deployment*. In INFOCOM 2007, 26th IEEE International Conference on Computer Communications, IEEE. 2007: 670-678.

[25] ASK Pathan, HW Lee, CS Hong. *Security in wireless sensor networks: issues and challenges*. In Advanced Communication Technology, 2006, ICACT, The 8th International Conference. 2006: 6-1048.

[26] R Szewczyk, J Polastre, A Mainwaring, D Culler. *Editors*. Lessons from a sensor network expedition. Springer. 2004: 307-322.

[27] K Sharma, M Ghose, D Kumar, RPK Singh, VK Pandey. A comparative study of various security approaches used in wireless sensor networks. *International journal of advanced science and technology.* 2010; 17: 31-44.

[28] MA Hamid, M Mamun-Or-Rashid, CS Hong. Routing security in sensor network: Hello flood attack and defense. *IEEE ICNEWS*. 2006: 2-4.

[29] M Čagalj, S Čapkun, JP Hubaux. Wormhole-based antijamming techniques in sensor networks. *Mobile Computing, IEEE Transactions*. 2007; 6: 100-114.

[30] C Karlof, N Sastry, D Wagner. *TinySec: a link layer security architecture for wireless sensor networks*. In Proceedings of the 2nd international conference on Embedded networked sensor systems. 2004: 162-175.
[31] Z Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks. *Real-World Wireless Sensor Networks*. 2005: 20-21.
[32] X Ma, DR Stinson, R Wei. Solution of an Optimization Problem Arising in the Analysis of Combinatorial Key Predistribution Schemes for Sensor Networks. 2014.
[33] CY Chen, HC Chao. A survey of key distribution in wireless sensor networks. *Security and Communication Networks*. 2014; 7: 2495-2508.
[34] N Farooq, I Zahoor, S Mandal. *Recovering from In-Band Wormhole Based Denial of Service.* In Wireless Sensor Networks. 2014.
[35] KSAS Mehak. Nature Based Trust Security Protocol against Greyhole Attacks in Opportunistic Networks. *Nature*. 2014; 1.