MAC Protocols Security in Wireless Sensor Networks: A Survey

[1]Ehsan Sharifi; [2]Mohammadreza Khandan
Taali Higher Education Institute of Information Technology
Qom, Iran
Email: Sharifi.eh89 {at} gmail.com

[3]Mahboobeh Shamsi
School of Electrical & Computer Engineering, Industrial University of Qom
Qom, Iran

Abstract— **Wireless Sensor Networks (WSN), is an Ideal Solution for variety of applications including surveillance, traffic control, environmental monitoring, battlefield surveillance and more. Current WSNs, are composed of hundreds or thousands sensor nodes that are distributed in a large environment, and often without surveillance. Sensor networks, developed by military applications motivation such as battlefield surveillance but nowadays, they are used in many non-military and industrial purposes. While the use of wireless networks in civil and military aspects is increasing, the need for security becomes necessity. Due to importance of Medium Access Control (MAC) protocols for providing security in WSNs, the main purpose of this paper is to survey recent research about the attacks on Medium Access Control protocols in WSNs and also resistance of these protocols against these attacks.**

Keywords- Wireless Sensor Network; Medium Access Control; Security.

I. INTRODUCTION

Wireless Sensor Networks (WSN) are networks that composed of many sensor nodes. The number of sensors varies depend on the scope of the network. The nodes of the WSN may be used in various environmental conditions, such as under the sea, battle or in a furnace. Sensor networks can be used for target tracking, system control and chemical and biological detection. In military applications sensor networks can enable soldiers to see around corners and to detect chemical and biological weapons long before they get close enough to cause harm them. Civilian uses of this network include environmental monitoring, traffic control and providing health care monitoring for the elderly while allowing them more freedom to move around [1]. This smart sensor nodes, have constraints on their power and memory. Generally WSNs work with the battery power. In addition, nodes may use other energy resources, such as solar energy or use vibration of their surroundings to become part of the required energy. However, the major problem with WSNs is limited energy.

Due to the limited energy and other properties of WSNs, protocols that designed for these networks must have low power consumption and support self-organization. These features are the main factors, but other factors such as fairness, delay and bandwidth efficiency should also be considered. Generally, we are faced with an equation for providing these factors and have to select the appropriate protocol.

Medium Access Control (MAC) protocols in WSNs, controls the accessing of channels in a network, so the highest number of nodes can share existing channels at the same time without affecting the accuracy of the data delivered to the indicated destination. Due to the wireless communication and insufficient resources and hard challenges in WSNs, an efficient MAC protocol is one of the most important factors which need to be considered before designing any WSN applications, to enhance the lifetime and improve the performance of the WSN [2]. Also, with regard to military and critical applications of WSN, we realized the importance of security of these protocols.

In this paper, we will survey the researches about providing WSNs security by secure MAC protocols and carry out a comparison between these protocols. In addition, we will study various attacks that target these MAC protocols and analyze performance of these protocols against these attacks.

II. SECURITY OF WSNS

Sensor networks have resource constraints in energy, memory, storage space and computing power. These constraints cause many challenges for WSNs designers and developers. The designers must design networks that are designed highly distributed, fault-tolerant, secure, and efficient in energy consumption.

For many sensor network applications, security requirements are very critical issue. Some of these applications are in the military field and must protect their important and critical data against attacks. Another major issue in these applications is data integrity and authentication. Apart from military applications, there are applications that authentication and integrity protection are more important than confidentiality in these networks. In many applications, these networks are used in hostile and inaccessible environments. Due to cost constraints, resistant and secure hardware using for all nodes is not possible. Therefore, the attacker can access any node and read nodes information that this information can include encryption keys. However in the WSNs Nodes coordinate is important to carry out their duties, in the event of loss any node

by other people, all of the WSN complex encounter with the problem. Therefore, to overcome these problems, we need the MAC protocols to provide Security of WSNs [3].

According to the characteristics of WSN, Short lifetime and its limited power resource compared to traditional networking, providing security in WSNs, is more different than the other networks. Traditional techniques like Diffie-Helman key agreement protocol or RSA Encryption systems Due to limited memory, low computational power and limited energy are not suitable for use in WSN. Symmetric encryption and cryptographic hashed functions in comparison with other algorithms, are faster and more efficient in terms of WSNs. Indeed in many activities about WSNs security, symmetric encryption is used.

III. SECURITY REQUIREMENTS IN WSNS

The security requirements of sensor networks can be summarized as follows:

A. *Data Confidentiality*

In the sensor network, nodes shall not disclose any data to neighbors. In many applications, nodes transmit very critical data, so create a secure communication channel in wireless sensor networks is very important. General information about the sensor, such as sensor identities and public keys, should be encrypted to be protected against traffic analysis attack.

Symmetric encryption with a secret key is a standard approach for data Confidentiality in WSNs. RC5 encryption system is a good solution to provide confidentiality in WSNs. Other Algorithms like DES that have high memory consumption and high computation need, is not suitable for WSNs.

B. *Data Integrity*

With data confidentiality, the adversary will not be able to steal information, but it does not mean that the data are secure. An adversary can alter the data, and cause irregularity in the network. Integrity ensures that the data that received during transmission is not changed by the malicious node. In the otherwise, even in the absence of malicious nodes, data can be modified, while is exchanged between nodes, so MAC using is necessary for providing data integrity.

C. *Data Authentication*

Due to the WSNs use wireless environment for data exchange, the network must have mechanism to specify source and destination identity. Otherwise, a malicious node can receive and send information to other nodes. Data authentication allows the receiver to be sure that data send from a valid sender that is a member of WSN. In the two-way communication, authentication can be obtained through a symmetric mechanism. Transceiver share a secret key to compute message authentication code (MAC) for all data.

D. *Data Freshness*

Even if the confidentiality and integrity of data is provided, the freshness of each message must to be provided. Simply, data freshness implies that the data is not old. This requirement, is more important when we use shared key strategies for the network. Although shared key distribution in the network is time consuming, but shared keys need to be changed. Also, if the sensor is aware of the key change time, it is easy to take down the sensor normal job. To solve this problem, we can add time sequence number to packets to ensure data freshness.

E. *Accessibility*

Accessibility, refers to providing WSNs service delivery at Denial of Service (DOS) attacks. DOS Attacks Can targets all layers of WSN and disable their Nodes. By DOS attack batteries or other power resources consume will be higher and much faster and causes failure in the nodes and network. Usually for providing accessibility in WSN, the redundancy of sensor nodes is used.

IV. MAC PROTOCOL DESIGN

MAC protocol must follow two targets in the sensor networks. The first objective is create a network infrastructure and second objective is a fair and efficient share of communication resources between sensor nodes. There are different expectations of good MAC protocol depending on the network structure, needs and abilities of the upper and lower layers. The following attributes must be considered for design efficient mac protocol: Environmental Accessibility, Reliability, Latency, Fairness, Energy Efficiency, Flow Control and Error Control [4].

Many peoples suggested different features for a good MAC protocol. Some of the most important of them as follow [5]:

In WSNs the first and matter issue is the lifetime of network and nodes. For this reason MAC protocols must provide Energy efficiency in WSNs. On the other hand, MAC protocol designer must consider network development, new nodes adding, multiplicity of nodes, the network topology changes and such topics. Other important issues related to MAC protocols are fairness, delay, throughput and bandwidth. Also all of these topics are important for the WSNs, but the most important thing is the lifetime of network nodes.

V. SECURITY OF WSN

One of the most significant current discussions in WSNs is the security of this network and it is becoming increasingly difficult to ignore the security of WSNs. For survey these researches we must study the attacks that target these networks. Generally these attacks are divided into the following categories by operation mode [6]:

A. *Attacks on Secrecy and Authentication*

Eavesdropping attack, modify or forgery packets and replay attacks are some of the attacks against secrecy and authentication. Standard cryptographic techniques can be used against these attacks.

B. *Attacks Against Availability of Network*

The overall goal of these attacks is a service disruption in the network. DOS attacks are the most important attacks on

WSNs availability and can have detrimental effects on the WSN.

C. Stealthy Attack

In a Stealthy attack, the attacker creates a network that contains Wrong data. For example, the attacker, get a node to inject false data and puts it in the network and thereby network contains the wrong data from this node.

D. Attacks Against Broadcast Authentication

Nodes must be able to authenticate the sender of the broadcasted messages. Conventional digital signature techniques, consume high energy and have delay. Less costly method against these attacks is μTESLA one-way key chain (the micro version of TESLA) [7] that consumes low energy. as noted, in the DOS Attacks Try to interrupt WSN service. For DoS attacks, the target resources may be file system space, process space, network bandwidth and network connections [8]. WSNs, are designed layered. For each layer, there is a special attack and each layer separately have action against tackles. But DOS attack is the only attack that can happen in every layer. For this reason more researchers work on this attack and the ways of protecting networks against these attacks. At physical layer the DoS attacks could be jamming and tampering, at the link layer, collision, exhaustion and unfairness, at the network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic [9]. For example, jamming attack usually is done by dropping the noise on one or more nodes. In fact Noise down here means the attacker sends the radio signals on a network that the frequencies of these signals have Interferences with the frequency of networks.

VI. Secure MAC Protocols

Secure MAC protocols are one of the most important issues in the WSNs. Many MAC protocols proposed for protecting WSN against threats, in the following, we'll survey some of this secure MAC protocols in following:

In The LEAP (Localized Encryption and Authentication Protocol) [10], each sensor uses four different keys that are, the individual key, group key, cluster key and Pairwise shared key. Individual key is shared key between the base station and sensor. Pairwise key shared between the two sensors. The cluster key shared between neighbors of sensors. The group key shared between all the sensors and base station use these keys to broadcasting in the network and also for providing data confidentiality in WSNs. Leap protocol uses a multi-broadcast authentication protocol, such as μTESLA so has loose synchronization and delayed authentication problems. This protocol protects WSN against node capture attack and prevent intrusions in the network. Also on this protocol, energy consumption depends on the number of nodes.

Multi-layer Perceptron Based Secure Media Access Control Protocol (MLP) [11] is the secure MAC protocol that proposed for protect border nodes in WSN. In this protocol DOS attack divided to collision Attack, injustice attacks resource consumption attack. MLP protocol depending on the attacks type and parameter changes, take action regarding to attacks.

These parameters that are very important for nodes are collision Rates (R_C) packet request rate (R_T) and the average waiting time for a packet (T_W). When the parameters have non-normal changes, MLP detects the attack and kind of attack. Subsequently, protocol, close physical and MAC layer and tries to provide security. Thereby with reducing in energy consumption, nodes lifetime increases. Studies have shown that under normal circumstances by changing in parameters, might the false alarms alert by MLP and cause performance decrease in network.

FSMAC [12] Protocol is the secure protocol for MAC that constructed on the CSMA / CA protocol. This protocol uses co-channels more fair and efficient than CSMA / CA, but this protocol seems weak against DOS attacks. In this protocol, each node can defend itself against attacks, and there aren't any central point for this task. In this protocol, DOS attacks divide to collision Attack, resource consumption attacks and unjustly attack. As a symbol, RTS by order show the arrival rate, the average waiting time and collision Overlap rates. Also, FSMAC protocol detects intrusions without any mistake.

Protocol that proposed by Shaheen et al. [13] is another effective MAC protocol. This protocol is a new approach for providing confidentiality and secure broadcast in wireless sensor networks that uses Time-varying keys. The heart of this approach lies in the use of a chain of keys and one key per packet. In this protocol, each packet is encrypted with a unique key and decryption key is the same. (i+1) key input in (i) packet and send to the sensor node. This protocol protects WSN against replay and node capture attacks. Despite the positive features of this approach, there is a risk that if one of the keys to be revealed any way, then all packets will be decoded.

TinySec [14] is the link layer protocol provides access control, message integrity and confidentiality for WSNs. This protocol is a part of official TinyOS release and uses a secure symmetric encryption key that shared between all nodes. This key has eternal life, and does not change from beginning to end of the establishment of the network connection. Although this protocol has remarkable simplicity and other advantage [15], but the simplicity and other advantages, cause network security reduction, because an adversary can prove the key in the long time. Moreover, an invalid sensor can send false data simply, and this approach is inherently vulnerable to replay attacks.

TinySec has two operating modes, first is TinySec-AE (Authenticated Encryption) and another is TinySec-Auth (Authenticated only). In TinySec-AE mode, TinySec, encrypts the data payload and confirmed packets by MAC (Message authentication code). In TinySec-Auth mode, TinySec authenticate packet by MAC and don't encrypt the data payload.

TinySec has low energy consumption and memory storage need. In fact this protocol adding less than 10% energy, latency, and bandwidth overhead, but hasn't acceptable

performance. In addition this protocol doesn't protect networks against node capture attack, however, guarantees the factors that needed for a secure connection, such as confidentiality, confirmation and message replay protection [16].

SPINS [7] Protocol that proposed by Adrian Perrig and et al. is formed from SNEP (sensor network encryption protocol) [17] and μTESLA secure building blocks. SNEP adds only 8 bytes to each message for providing secure point-to-point communication that is a bit redundant. Also, by providing semantic security, eliminates the possibility of eavesdropping attack on encrypted messages. In addition by message authentication code (MAC), guarantees packet receiving by the recipient if the packet send by valid sender. This protocol protected against replayed messages by using counter values in message authentication code, and thus the network is robust against replay attacks.

In the μTESLA [7] some features have been added to standard TESLA to solve some problems in the WSNs and provide efficient broadcast authentication. This method uses time-varying keys for guaranties data authentication. Also data integrity is achieved by message authentication code values that generated by secret key and appended to the data.

SenSec [18] protocol is a link layer protocol and similar to Tinysec protocol. While the Tinysec use 2 work modes, SenSec Works in one mode and work similar to the Tinysec-AE. By using SenSec protocol, in some cases we have seen a reduction in energy consumption and security. Also MAC calculating cost in this protocol has been reduced. By many-keying mechanism, this protocol protects the network against many types of attacks. Moreover by this mechanism, in some cases, the network is resilient against node capture attack. By using the skipjack-X cipher block encryption scheme in SenSec, This protocol is more resistant against resource consumption attack compared to Tinysec protocol that uses skipjack. Furthermore, this protocol has good performance against Brute Force attacks.

MiniSec [16] protocol is a secure mac protocol in the network layer. This protocol uses Tinysec protocol's features with minor modification, such as adding a sequence number to protect the network against replay attack. MiniSec consumes lower energy than TinySec, but the level of security is equivalent or more than ZigBee. This protocol like Tinysec protocol uses shared public key for all the sensors and for this reason inherits weaknesses of Tinysec. MiniSec offers higher replayed attack protection over other security protocols without transmission overhead or problems related to countering synchronization [1]. This protocol uses offset codebook (OCB) encryption system.

In MiniSec protocol there are two operating modes. First is MiniSec-U that unicast packet and another mode that publishes all packets in broadcast mode, is called MiniSec-B. Both modes use OCB encryption system and provide semantic security.

TE_2S [19] protocol proposed by Ching-Tsung Hsueh et al. and Provides MAC security by Cross-layer approach. This protocol designed to protect the WSNs against Power Exhausting attack. In this protocol, 2 layer communication protocol is presented. In the first layer, the session key agreement is done and in the second layer data delivery is done. By using this protocol, the authentication time is tremendously reduced. Thus, in this protocol the effects of attacks that consume energy, is reduced according to the energy analysis. In addition, this protocol protects network against replay and spoofing attacks with more efficient energy consumption.

VII. SUMMARY AND CONCLUSIONS

Due to the properties and physical characteristics of WSNs, security are the One of the most important issues in the MAC protocols and in recent researches, security considered inside the other important issues of the WSNs. In this regard, Table 1, shows secure and efficient MAC protocols and attacks that these protocols protect WSN against those.

TABLE I. SECURE MAC PROTOCOLS AND THEIR FEATURES

Protocols	Features	Attacks protected
Leap	Using multiple keys	Intrusions, Node Capture
MLP	Rapid detection of attack by changing the parameters, Guarantee security by closing physical layer and MAC	DOS
FSMAC	The lack of a central control structure, Nodes self-protection	DOS
Shaheen	Ensure confidentiality by time-varying keys	Replay, Node Capture
Tinysec	Easy to use, Provide integrity and confidentiality	Replay
SPINS	Prevent Eavesdropping attack by semantic security, Providing confidentiality, Integrity, and freshness	Replay, Eavesdropping
SenSec	Protect WSN against many types of attacks by many-keying mechanism	Replay, Brute force
MiniSec	Provide semantic security, without overload	Replay
TE_2S	Reduce impact of power resource consumption attack by reducing time of authentication process	Replay, Spoofing, Forgery, Energy consumption, Sleep Deprivation.

According to the table, MLP and FSMAC protocols protect WSNs against DOS attacks. In The MLP protocol Due to the variation of the basic parameters of the network, attack has been detected and depending on the type of attack, physical layer or MAC is disabled and Security is provided.

SPINS Protocol protect WSN against the replay and eavesdropping attacks, guarantees confidentiality and integrity. TinySec Protocols protect WSN against replay attacks, and guarantees confidentiality and integrity in WSN. SenSec protocol Similar to the TinySec and moreover, by many-

keying mechanism detect the type of attack and Protect WSN. In protocol that presented by Shaheen and others, WSNs confidentiality provided by time-varying keys.

MiniSec Protocol provides semantic Security, moreover has lower energy consumption compared to TinySec. Leap protocol provides security by multiple keys and protect WSN against intrusions and anomalies. Finally, the TE_2S protocol protects WSN against replay, energy consumption and sleep deprivation attacks with the energy efficiency.

REFERENCES

[1] A.-B. García-Hernando, J.-F. Martínez-Ortega, J.-M. López-Navarro, A. Prayati, and L. Redondo-López, WSN Application Scenarios: Springer, 2008.

[2] M. Atto and C. Guy, "Wireless Sensor Networks: MAC Protocols and Real Time Applications," in The 13th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2012)(PGNet2012), Liverpool, UK, United Kingdom, 2012, pp. 1-6.

[3] H. Ng, M. Sim, and C. Tan, "Security issues of wireless sensor networks in healthcare applications," BT Technology Journal, vol. 24, pp. 138-144, 2006.

[4] R. Yadav, S. Varma, and N. Malaviya, "A survey of MAC protocols for wireless sensor networks," UbiCC journal, vol. 4, pp. 827-833, 2009.

[5] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," Networking, IEEE/ACM Transactions on, vol. 12, pp. 493-506, 2004.

[6] E. Shi and A. Perrig, "Designing secure sensor networks," Wireless Communications, IEEE, vol. 11, pp. 38-43, 2004.

[7] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless networks, vol. 8, pp. 521-534, 2002.

[8] Q. Ren, Medium Access Control (MAC) Layer Design and Data Query Processing for Wireless Sensor Networks: ProQuest, 2007.

[9] D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv:0909.0576, 2009.

[10] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," ACM Transactions on Sensor Networks (TOSN), vol. 2, pp. 500-528, 2006.

[11] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in Neural Networks, 2009. IJCNN 2009. International Joint Conference on, 2009, pp. 1680-1687.

[12] Q. Ren and Q. Liang, "Fuzzy logic-optimized secure media access control (FSMAC) protocol wireless sensor networks," in Computational Intelligence for Homeland Security and Personal Safety, 2005. CIHSPS 2005. Proceedings of the 2005 IEEE International Conference on, 2005, pp. 37-43.

[13] J. Shaheen, D. Ostry, V. Sivaraman, and S. Jha, "Confidential and secure broadcast in wireless sensor networks," in Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on, 2007, pp. 1-5.

[14] C. Karlof, N. Sastry, and 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, pp. 162-175.

[15] J. F. Kurose and K. W. Ross, Computer networking: Pearson Education, 2012.

[16] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on, 2007, pp. 479-488.

[17] L. Tobarra, D. Cazorla, and F. Cuartero, "Formal analysis of sensor network encryption protocol (snep)," in Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on, 2007, pp. 1-6.

[18] I. Krontiris, T. Dimitriou, H. Soroush, and M. Salajegheh, "WSN link-layer security frameworks," Wireless Sensor Network Security, vol. 1, p. 142, 2008.

[19] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks," in Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on, 2011, pp. 258-263.