International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

A Comparative Study of Security protocols in Wireless Sensor Networks

J. Rosy Mary*, N. Kannammal
Department of Computer Science, Holy Cross College(Autonomous),Tiruchirappalli Tamil Nadu, India

ABSTRACT

Wireless sensor networks is composed of large number of nodes that have capabilities to sense their surroundings, perform computations and communicate wirelessly to their neighbor nodes and base station. Wireless sensor networks (WSNs) are one of the most interesting research areas and have become very popular technology. This paper addresses the various Security protocols, also related work done so far in the field of security in Wireless Sensor Networks (WSNs).

Keywords : Wireless Sensor Network, Architecture, Sensor Network Protocol Stack, Security, Requirements, Applications and Security.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure less wireless networks to monitor physical or environmental conditions, and consists of various types of sensors, Shown in Fig.1 to assemble the information such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink.

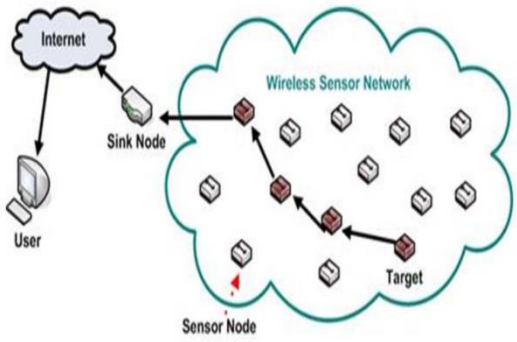

Figure 1: Wireless Sensor Network

Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them.

Depending on the environment, the types of networks are decided so that those can be deployed underwater, underground, on land, and so on. Different types of WSNs include Terrestrial WSNs, Underground WSNs, Underwater WSNs, Multimedia WSNs and Mobile WSNs. This article gives details of various applications of Wireless Sensor Networks and security protocols, also related work done so far in the field of security in Wireless Sensor Networks (WSNs).

II. RELATED WORK IN SECURITY

Abd El dayem et al[1] proposed a security protocol for message and entity authentication.They introduced a development key distribution schemes in very possible way and less time computation than other protocols. The proposed protocol considers nobile nodes, so they introduced an efficient re-authentication protocol. This

protocol is more efficient than other protocols in security.

Sai Teja Kadiyala et al[4] analyzed the security issues and finds the possible techniques to minimize the effect of the threats, especially the privacy, on the sensitive patient's data. The data that is transmitted through the cloud is vulnerable to various security attacks. One of the primary security threats is privacy. Data privacy aims at protecting the sensitive information and not revealing this information to the unauthorized entities.

The anonymization techniques, namely the Generalization and Suppression are conducted on the large data sets which are clustered using hierarchical clustering. The research in future can be a scalable approach on large data sets where the patient's data can be organized in an efficient manner, and the privacy of the sensitive data can also be preserved.

Sharan Kumar Vaddadi et al[5] implemented the DiDrip protocol. This protocol is used to secure and convey Data discovery and dissemination protocol. Dissemination protocols are essential in light of the fact that all WSNs are conveyed in unfriendly situations and accordingly manual reinventing of such nodes is impractical. Numerous data dissemination protocols have been presented with time and every one of them help in dissemination of program code, design parameters, questions, charges, mass data and so onwards.

Jia Zhu et al[6] discussed techniques of improving the wireless physical-layer reliability in the face of interference, path loss, fading and link failure. Next, wireless jammers and eavesdroppers have been reviewed along with their countermeasures for the sake of guaranteeing communications security in IWSNs. And also discussed the tradeoff between the security and reliability of wireless sensor-sink transmissions, where the security and reliability are, respectively, quantified in terms of the outage probability experienced at the sink and the intercept probability encountered at the eavesdropper.

III. WSN ARCHITECTURE AND PROTOCOL

The most common WSN architecture follows the OSI architecture Model is given in Fig.2. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task management. These layers of the WSN are used to accomplish the n/w and make the sensors work together in order to raise the complete efficiency of the network.

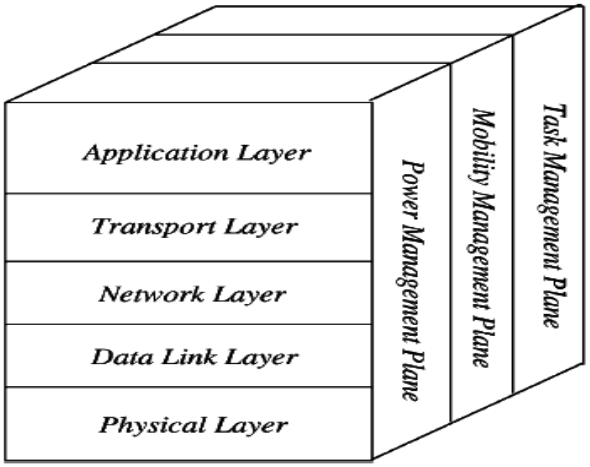

Figure 2: Sensor Network Protocol Stack

Physical layer

The physical layer addresses the hardware detail of wireless communication mechanism. This layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption.

Data Link Layer

The data link layer is concerned with the media access control (MAC) protocol. Since the wireless channel is susceptible to the noise and sensor nodes may be changing the location MAC protocol at the data link layer has to be power-aware and should have the capability of minimizing the collisions.[3]

Network Layer

The network layer manages the routing the data supplied by the transport layer or between the nodes. Whereas the transport layer is able to maintain the data flow if the WSN application requires that. Various type of application can be implemented in the application depending the physical environmental sensing.

The wireless sensor networks defined three management plan named power, mobility and task management. These plans are responsible for monitoring the power, movement and task distribution among the sensor nodes. These management plans helps the sensor nodes to coordinate sensor tasks and minimize the overall power consumption.

IV. APPLICATIONS OF WSN

There are numerous applications of WSNs in industrial automation, traffic monitoring and control, medical device monitoring and in many other areas. Some of applications are discussed below:

Disaster Relief Operation

If an area is reported to have been stricken from some sort of calamity such as wildfire, then drop

the sensor nodes on the fire from an aircraft. Monitor the data of each node and construct a temperature map to devise proper ways and techniques to overcome the fire.

Military Applications

As the WSNs can be deployed rapidly and are self organized therefore they are very useful in military operations for sensing and monitoring friendly or hostile motions. The battlefield surveillance can be done through the sensor nodes to keep a check on everything in case more equipment, forces or ammunitions are needed in the battlefield.

The chemical, nuclear and biological attacks can also be detected through the sensor nodes. An example of this is the 'sniper detection system' which can detect the incoming fire through acoustic sensors and the position of the shooter can also be estimated by processing the detected audio from the microphone.

Environmental Applications

These sensor networks have a huge number of applications in the environment. They can be used to track movement of animals, birds and record them. Monitoring of earth, soil, atmosphere context, irrigation and precision agriculture can be done through these sensors. They can also used for the detection of fire, flood, earthquakes, and chemical/biological outbreak etc. A common example is of 'Zebra Net'. The purpose of this system is to track and monitor the movements and interactions of zebras within themselves and with other species also.

Medical Applications

In health applications, the integrated monitoring of a patient can be done by using WSNs. The internal processes and movements of animals can be monitored. Diagnostics can be done. They also help in keeping a check on drug administration in hospitals and in monitoring patients as well as doctors. An example of this is 'artificial retina' which helps the patient in detecting the presence of light and the movement of objects. They can also locate objects and count individual items.

Home Applications

As the technology is advancing, it is also making its way in our household appliances for their smooth running and satisfactory performance. These sensors can be found in refrigerators, microwave ovens, vacuum cleaners, security systems and also in water monitoring systems. The user can control devices locally as well as remotely with the help of the WSNs.

V. SECURITY REQUIREMENT

Since sensor networks are used for many applications where security is crucial. It is essential to ensure secure communication among the nodes. It is not possible to use general secure communication techniques for WSNs because of resource-constraints and communication overheads involved. The security requirement of wireless sensor network can be classified as follows:

Authenticity

Authentication is important application in sensor networks. Adversary can easily inject messages, the receiver needs to ensure that data used in any decision making process originate from trusted source. Authentication allows sender node and receiver must be sure that they talking really to the node to which they want to communicate.

Confidentiality

Confidentiality guarantee that data sent on the channel will not be read correctly by anybody other than communicating nodes. For this purpose, the message is sent on the channel in

encrypted form. Confidentiality means keeping information secrete from unauthorized parties.

Integrity

Integrity means that the data should not be modified by adversary to the receiver. If it happens, then receiver must verify that data received is exactly the same as sent by the sender. For that purpose, a message

authentication code (MAC) is generated by the sender using some MAC key and that is sent with the encrypted message. At the other end, the receiver will verify the authenticity of the received message by using that MAC key.

Scalability

The key management scheme, should be scalable in the sense that if network size grows, it should not increase the chances of node compromise, should not increase communication overhead. It should allow nodes to be added in network after the operation as well.

VI. SECURITY PROTOCOLS

SNEP

Semantic security: Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats within the lifetime of the node.

Data authentication: If the MAC verifies correctly, a receiver can be assured that the message originated from the claimed sender.

Replay protection: The counter value in the MAC prevents replaying old messages. Note that if the counter were not present in the MAC, an adversary could easily replay messages.

Weak freshness: If the message verified correctly, a receiver knows that the message must have been sent after the previous message

it received correctly (that had a lower counter value). This enforces a message ordering and yields weak freshness.

Low communication overhead: The counter state is kept at each end point and does not need to be sent in each message.

µTESLA

µTESLA provideS secure communication channels using only symmetric cryptography in sensor networks. This protocol offers following properties:

- Confidentiality
- Authentication
- Integrity
- Freshness
- Low overhead

SPINS

According to various requirements of WSN security, SPINS offers two kinds of protocol: SNEP and µTESLA to secure communication channels. SNEP protocol offers

- data confidentiality
- data Integrity
- data authentication
- freshness of weak message
- protection of replay message.

A common solution to accomplish message authenticity and integrity is to employ a Message Authentication Code (MAC), which is added along with a message as a signature. The SNEP protocol seems to be feasible for WSN due to the function of the MAC value. The requirements of µTESLA are as follows: (a) base station and sensor nodes should be loosely time synchronized, and (b) each and every node has upper bound information on high time synchronization error. There is a need for more

investigations to implement on various modulation approaches of transceiver unit in the sensor nodes. Moreover, the memory must be with maximum computation speed and energy unit.

LEAP

In WSNs, LEAP offers multiple keying mechanisms to provide confidentiality and authentication. Based on the different criteria, the packets exchanged by nodes in WSN can be categorized into various classes.

LEAP supports the establishment of four kinds of key: an individual key shared with the BS, a pairwise key shared with the other WSNs, a cluster key shared with several neighboring nodes, a group key shared by all the nodes in the network. The major benefits of the LEAP protocol are as follows: (a) comprising µ-TESLA, one-way key chain authentication, key revocation, and key refreshing, scalability, and being

able to accomplish cluster communications. The drawback of this scheme is that it assumes that sink node is never compromised.

TINYSEC

Karlof et al. designed the replacement for the unfinished SNEP, known as TinySec (2004) [17]. Inherently it provides similar services, including authentication, message integrity, confidentiality and replay protection. A major difference between TinySec and SNEP is that there are no counters used Proceedings of the Third International Conference on Wireless and Mobile Communications (ICWMC'07) 0-7695-2796-5/07 $20.00 © 2007 in TinySec. Bandwidth, latency and power consumption are Bandwidth, latency and power consumption are analyzed for TinySec analyzed for TinySec „ It is feasible to implement this in software It is feasible to implement this in software.

ZigBee

This device allows other devices to join the network and also distributes the keys. There are three roles played: trust manager, whereby authentication of devices requesting to join the network is done, network manager, maintaining and distributing network keys, and configuration manager, enabling end-to-end security between devices. It operates in both Residential Mode and Commercial Mode. The Trust Center running Residential Mode is used for low security residential applications. Commercial Mode is designed for high-security commercial applications. The following Table 1 explains the security protocols and their security requirements.

TABLE I. Security Protocols and their Requirements

Protocols	Security Requirements				Additional Features
	Authenticity	Confidentiality	Integrity	Scalability	
SNEP	✓	✓	✓	-	Freshness, Low overhead
µTESLA	✓	✓	✓	-	Freshness, Low overhead
SPIN	✓	✓	✓	-	freshness of weak message, protection of replay message,
LEAP	✓	✓	✓	✓	key revocation, key refreshing
TINYSEC	✓	✓	✓	-	Bandwidth, latency, power consumption
ZIGBEE	✓	✓	✓	-	improve network, security layers

- To measure the scalability of protocols for WSN.
- To identify the protocols which provide scalability as important feature.
- To enhance existing protocols with scalability.

VII. CONCLUSION

This study presents various security protocols of WSN using their security requirements. Even though the security protocols are increasingly being adopted for WSN, enhancing the scalability for the protocol is still a difficult task. There is a need for enhancing the protocol with scalability.

VIII. REFERENCES

[1] Sanaa. S.Abd El dayem, M.A.Mokhtar,M.R.M.Rizk, "Security for Wireless Sensor Network", In:Proc. Of 6th

International Conference on Information Communication and Management, IEEE, 2016.

[2] Ghasem Farjamnia and Yusif Gasimov,"Wireless Sensor Networks Architecture" International Research Journal of Computer Science, January 2016.

[3] Swati Bartariya, Ashutosh Rastogi," Security in Wireless Sensor Networks: Attacks and Solutions",International Journal of Advanced Research in Computer and Communication Engineering, March 2016.

[4] Sai Teja Kadiyala, Anusha Sowdhari, Sowmya Valina, Sajeesh Pandhaloor, Harrison Osula, "Security/Privacy in Health Care Monitoring Using Wireless Sensor Networks", University of Bridgeport.

[5] Sharan Kumar Vaddadi, B Krishna, "Ensuring Distributed Data Discovery By Providing High Security In Wireless Sensor Networks", International Journal of Mechanical Engineering and Computer Applications.2016.

[6] Jia Zhu, Yulong Zou and Baoyu Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks", 2017.

[7] S.R.Boselin Prabhu, M.Pradeep, E.Gajendran, " Military Applications Of Wireless Sensor Network System", Multidisciplinary Journal of Scientific Research & Education, 2(12), December-2016,

[8] A. J. Albarakati, "A Study on Underwater based Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 119 – No.12, June 2015.

[9] K. Gupta, V. Sikka, "Design Issues and Challenges in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 112 – No 4, February 2015.

[10] Danilo de Oliveira Gonçalves and D.G. Costa, "A Survey of Image Security in Wireless Sensor Networks", J. Imaging 2015.

[11] Bushra Rashid, Mubashir Husain Rehmani, "Applications of wireless sensor networks for urban areas: A survey", Journal of Network and Computer Applications, September 2015.

[12] Kamaldeep Kaur, Parneet Kaur, Er. Sharanjit Singh, "Wireless Sensor Network: Architecture, Design Issues and Applications", International Journal of Scientific Engineering and Research, November 2014.

[13] X. Huang, M. Ahmed, D. Sharma, "Timing Control for Protecting from Internal Attacks in Wireless Sensor Networks", IEEE, ICOIN 2012, Bali, Indonesia, February 2012.

[14] Muhammed R Ahumed, Xu Huang, Dharmandra Sharma, and Hongyan Cui, Wireless Sensor Network: Characteristics and Architectures", World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 2012.

[15] Saurabh Singh, Harsh Kumar Verma, "Security For Wireless Sensor Network", International Journal on Computer Science and Engineering, Vol. 3 No. 6 June 2011.

[16] T. He, J. A. Stankovic, C. Lu, T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks", In: Proc. of 23rd Int'l Conf. on Distributed Computing Systems. Rhode Island: IEEE Computer Society, 2003.

[17] Karlof, "TinySec: a link layer security architecture for wireless sensor networks", SenSys '04,2nd International conference on Embedded networked sensor systems.2004.