Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A-SURVEY SECURITY PROTOCOL FOR WIRELESS SENSOR NETWORK

PALAK J CHAUHAN[1], KUNAL M PATTANI[2]

[1]M.E. (E.C.) Student, [2]Professor
[1,2] C.U. Shah College of Engineering and Technology, Wadhwan City Gujarat.

Abstract-- Nowadays, Wireless Sensor Networks are emerging because of the technological developments in Wireless Communication. Wireless Sensor Networks are deployed mostly in open and unguarded environment. The key features of Wireless Sensor Networks are low power, low-memory, low-energy scaled nodes. Security is a fundamental requirement for Wireless Sensor Network. Security is the main concern for everything whether it is for wired based network or wireless based network. Security in Wireless Sensor Network plays an important role in node communication. For Wireless Sensor Network so many security protocol available but some have some limitation. In this paper, our center of attention is security protocols for Wireless Sensor Network through this paper; we have to identify the security protocols and their limitation for Wireless Sensor Network.

I. INTRODUCTION

A Wireless Sensor Network [1] is a wireless network consisting of large populations of specially distributed sensor nodes to cooperatively monitor physical or environmental condition [2]. A sensor is device that has sensing and receiving capability to sense and receive a signal and react to that signal in individual manner. Wireless Sensor Network consist many sensor node which are limited in computation, less memory space and small in size. Self-organizing and self-configuration are the special feature of this network. Wireless Sensor Network is vulnerable to various attacks. So that's why security must in Wireless Sensor Network. Security has contained that the attacks and monitoring on Wireless Sensor Network. Wireless Sensor Network [1] has contain several sensor nodes and actuators are highly distributed. Due to the high distribution only security is very much needed in the network. So, here discussion based on security protocol for Wireless Sensor Network. Secure wireless sensor network, security must be integrated into every node of the system. This is due to the possibility that a component implemented without any security could easily become a point of attack. This dictates that security must pervade every aspect of the design of a wireless sensor network application that will require a high level of security [4]. In this paper, section 2, we discussed about security in WSN. In section 3, we discussed about security protocol like SNEP, µTESLA, SPIN. In section 4, shows limitations in existing security protocol.

II. SECURITY IN WSN

The security in wireless sensor network is essential and their main objective is to maintain the data freshness, self organization, synchronization of time, protected localization, cost efficiency, self healing . Challenges in Security for wireless sensors are to retain the security against standard resources, untrusted communication and unattended operation [6][8]. The constraints for node in sensor network are to have high energy, storage, memory and processing speed. The wireless networks are unreal, having collision and latency and lack of physical infrastructure and remotely

managed. The common attacks like interruption, modification, fabrication are frequently occurs in the networks. Security threats in sensor network are most importantly focused on authentication, availability and certifications. In this, they perform the attacks like modification, forgery, deletion and replay attack [2].

III. SECURITY PROTOCOL

Wireless network are more vulnerable to security attacks than wired network. The sensor nodes are low power devices with limited computational and communication resources [1]. The network is more exposed to attacks because they are deployed in untrusted location area. Asymmetric digital signatures for authentication are impractical because it requires high communication strategy with high power. Deployment of security mechanisms creates additional overhead like having consumed energy, increases latency. Due to this the lifetime of the network is directly decreases. In the real time environment, there are a number of security protocols existed. The important protocols are described in this paper [3].
SNEP: Secure Network Encryption protocol.
µTESLA: Micro version of Timeed, Efficient, Streaming, Loss-Tolerant, Authentication protocol.
SPINS: Sensor Protocol for Information via Negotiation.

3.1. SNEP

The strength of SNEP (Secure Network Encryption Protocol) provides secure end-to-end communication [4]. These protocols are having the following properties: data confidentiality, authentication, integrity, and freshness. Data confidentiality is one of the most basic security primitives and it is used in almost every security protocol. A simple form of confidentiality can be achieved through encryption, but secure encryption is not sufficient. Another important security property is semantic security. For example, even if an attacker has an encryption of a 0 bit and an encryption of a 1 bit, it will not help to distinguish whether a new encryption is an encryption of 0 or 1[6][8]. The basic technique to achieve this is randomization: Before encrypting the message with a chaining encryption function, the sender precedes the message with a random bit string. This prevents the attacker from inferring the plaintext of encrypted messages if it knows plaintext-ciphertext pairs encrypted with the same key.

SNEP offers the following properties [6]:

- Semantic security. Since the counter value is incremented after each messages, the same message is encrypted differently each time. The counter value is sufficiently long enough to never repeat within the lifetime of the node.
- Data authentication. If the MAC verifies correctly, a receivers knows that the message originated from the claimed sender.
- Replay protection. The counter value in the MAC prevents replay of old messages. Note that if the counter were not present in the MAC, an adversary could easily replay messages.
- Weak freshness. If the message verifies correctly, a receiver knows that the message must have been sent after the previous message it received correctly. This enforces a message ordering and yields weak freshness.

3.2 µTESLA

µTESLA- micro version of Timed, Efficient, Streaming, Loss-Tolerant, Authentication protocol.

The recently proposed TESLA protocol provides efficient authenticated broadcast. However, TESLA is not designed for the limited computing environments we encounter in sensor networks for the following three reasons [8]:

Standard TESLA has an overhead of approximately 24 bytes per packets. For networks connecting workstations this is usually not important. Sensor nodes, however, send very small messages that are around 30 bytes long. It is basically impractical to disclose the TESLA key for the previous intervals with every packet: with 64 bit keys and MACs, the µTESLA-related part of the packet would constitute over 50% of the packet.

We design µTESLA to explain the following inadequacies of TESLA in sensor networks [8]:

- TESLA authenticates the initial packet with a digital signature, which is expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for sending and receiving. µTESLA disclose the key once per epoch.
- It is expensive to store a one-way key chain in a sensor node. µTESLA restrict the number of authenticated senders.

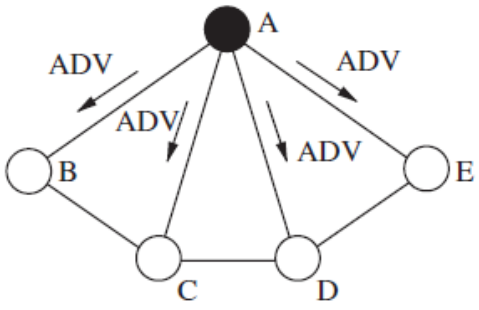
3.3 SPINS

SPIN – Sensor protocol for Information via Negotiation.

SPIN [1] is a data-centric routing protocol. The sensor nodes negotiate with each other before transmitting the actual data using meta-data. Nodes in this network use a high level name to describe their collected data is called meta-data [5]. It is basically three-way handshake protocol which are ADV, REQ, and DATA. Problems like implosion and overlapping are solved by negotiation thus they achieving energy efficiency. The SPIN family protocols include many protocols. They are SPIN-PP, SPIN-EC, SPIN.BC, SPIN-RL.

SPIN-PP

This protocol designed for a point to point communication [7]. In this protocol two nodes can communicate with each other without interfering with other nodes. SPIN node receives a new data, it broadcasts an ADV message to its neighbor nodes, it contains the meta-data. If the neighbor does not have the data and needs the data, it sends a REQ message to request data stating which advertised data it wants and does not want. DATA is the actual message which is sent to the requesting node. This way the entire sensor area will receive a copy of the data.



(a)

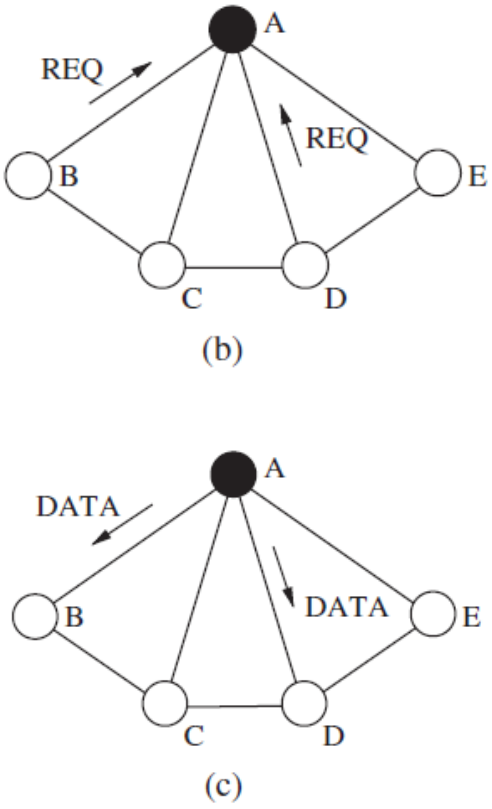


Figure 1. The SPIN-PP Protocol: (a) Advertisement Phase, (b) Request Phase, and (c) Data Transmission [7].

SPIN-EC

This protocol designed for energy Conversation. The sensor nodes communicate using the same three-way handshake protocol as in case of SPIN-PP. If it is above the energy threshold it will perform the operations similar to SPIN-PP. If it is below the threshold energy it will not send the REQ message and hence will not participate in the communication. [7]

SPINS-BC

This protocol is designed for broadcast channels nodes. When a node sends out a message, it is received by every node irrespective of the message destination. If a node wishes to send a message and senses that the channel is currently in use, it must wait for the channel to become idle before attempting to send the message. Therefore it wastes both time and energy [7]. However, the advantage of such networks is that when a single node sends a message out to a broadcast address, this message can reach all of the nodes neighbors using only one transmission.

SPIN-RL

This protocol is designed for reliable nodes. It is similar to SPIN-BC protocol. Each node keeps track of all the advertisements and the nodes sending them. If it does not receive any requested data within a certain period of time, it sends out the request again.

IV. LIMITATION IN EXISTING SECURITY PROTOCOLS

The security protocol having some limitations which are following below:

1. Overload in communication
2. Low computational power
3. High Resource consumption

4. Lack of integrity
5. Lack of confidentiality

V. CONCLUSION

This paper contained overview of security protocol for Wireless Sensor Network. Nowadays security is one of the most important issue in Wireless Sensor Network. So,this paper make to more understand about the general requirement of security and attacks on Wireless Sensor Network.

REFERENCES

1. I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A Survey", 1389-1286/02/$ - see front matter _ 2002
2. Dr.Yingying, Dr. Ban-Othman, Dr. Rahul Vaze, "Call for papers Ad-hoc and Sensor Networking Symposium",IEEE GLOBECOM 2014.
3. P.S RAMESH1, F. EMILY MANOZ PRIYA2, B.SANTHI**, "**REVIEW ON SECURITY PROTOCOLS IN WIRELESS SENSOR NETWORKS", Journal of Theoretical and Applied Information Technology, 2012.
4. Fasee Ullah, Masood Ahmad, Masood Habib, Jawad Muhammad "Analysis of Security Protocols for Wireless Sensor Networks", 978-1-61284-840-2/11 ©2011 IEEE.
5. Debnath Bhattacharyya, Tai-hoon Kim ,and Subhajit Pal, "A Comparative Study of Wireless Sensor Networks and Their Routing Protocols", SENSOR ISSN 1424-8220, 2010.
6. ADRIAN PERRIG, ROBERT SZEWCZYK, J.D. TYGAR, VICTORWEN and DAVID E. CULLER, "SPINS: Security Protocols for Sensor Networks", Wireless Networks 8, 521.534, 2002.
7. Kalpana Sharma, Neha Mittal and Priyanka Rathi, "Performance Analysis of Flooding and SPIN in Wireless Sensor Networks" ,International Journal of Future Generation Communication and Networking,2014.
8. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar**, "**SPINS: Security Protocols for Sensor Networks", *Mobile Computing and Networking* 2001.

