"International Journal for Science and Emerging Technologies with Latest Trends" 4(1): 42-48 (2012)

ISSN No. (Online):2250-3641
ISSN No. (Print): 2277-8136

SURVEY ON PRE-SHARED KEY IN WIRELESS SENSOR NETWORK

Madhuri Prashar* and Rajeev Vashisht**

Department of Computer Science Engineering,, DAVIET Jalandhar

(Received 05 December 2012 Accepted 14 December 2012)

Abstract- This paper presents the overview of key management ,and Pre-shared key scheme in WSN,then this paper presents implementation of Pre-shared key Protocol using different parameters and shows communication of nodes Based on the results of its implementation, some limitations of PSK are explained.

Keywords –WSN,Pre-shared key scheme in WSN,Enegy efficiency of WSN,Connectivity of WSN.

1.Introduction

A wireless sensor network is a network which consists of a number of sensor nodes that are wirelessly connected to each other. These small, low-cost, low-power, multifunctional sensor nodes can communicate in short distances. Each sensor node consists of sensing, data processing, and communication components. A large number of these sensor nodes collaborate form wireless sensor networks.[1] A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. To ensure scalability and to increase the efficiency of the network operation, sensor nodes are often grouped into clusters [2 ,3]

Wireless networks are networks which provide users with connectivity regardless of their actual physical location. Wireless networks are networks that do not involve cables. It is a technique that saves the cost of cables for networking and helps entrepreneurs and telecommunication networks in specific premises in their installations. The transmission system is usually implemented and administrated via radio waves where the implementation takes place at physical level.

2.Key management in wsn

In this paper, we present wireless sensor network key management survey for PSK/ Preloaded scheme and related topics on key management and further we improve its limitations through our proposed scheme.

Key management is an important issue in the security of WSN. It actually helps in maintaining the confidentiality of secret information from unauthorized access. Furthermore, it is used for verifying the integrity of exchanged messages and authenticity of the sender.

2.1 Typical *Key Management Goals*:

- The protocol must establish a key between all sensor nodes that must exchange data securely
- Node addition / deletion should be supported
- It should work in undefined deployment environment
- Unauthorized nodes should not be allowed to establish communication with network nodes [7].

2.2 *Main features of Key Management in Wireless Sensor Networks*

- Confidentiality- Nodes must not reveal data to any unauthorized access.
- Integrity- The data must not be changed between transmission due to environmental activity.
- Data Freshness – The old data should not be behaved as a new one.
- Authentication- The data which is used in decision making process must originate from correct source.

- Robustness - When some nodes in the network of WSN are compromised then the entire network should not be compromised.
- Self - Organization- It mainly considers with flexibility of nodes to be self organizing (autonomous) and self – healing (failure tolerant).
- Availability- The network should be for appropriate interval of time.
- Scalability. [8]

2.3 *Limitations of Various Key Management Scheme in Wireless Sensor Networks*

- Network Keying: Lacks of Robustness.
- Pair-wise Keying:
  a) Non –scalable.
  b) Unable to self organize.
  c) Not flexible.
- Group Keying:
  a)Lacksof efficient storage for group keying in IEEE 802.15.4.
  b) Difficult to secure set up.
  c) Clusterinformation is application dependent.[7,8]

2.4 *Key Management Process*

Key is the most important component for most of the Cryptographic algorithms. Keys are generally numbers randomly selected from a large set of numbers. Management of these keys are very important in cryptography. Management of keys include the following:

(i)*Key Generation*: It is the process in which a pool of key are generated. It is done in offline mode by a trusted authority.

(ii)*Key Establishment*: It is the most important phase of key management process. Key establishment is the process by which right keys for right users can be determined and key rings for each user are sent to them accordingly.

Key establishment can be done in many ways. Trusted Authority can help in sending the keys to each user through a secure channel. But this mechanism is a costly one and does not suit for sensor networks. So, in sensor networks Key Pre-distribution is used in which key rings are installed in the nodes before deployment of network in offline mode.[19]

Key establishment process in Wireless sensor networks mainly consists of three phases.

(i)*Key pre-distribution* : Pre-loading keys in sensor nodes prior to deployment. The keys present in a sensor node constitute the key ring of the sensor.

(ii)*Shared key discovery* : To find a common shared key between two communicating nodes.

(iii)*Path key establishment* : If a common key does not exists, then a path has to be found between the communicating nodes. A path key is then established between the communicating nodes.

In Key Pre-Distribution scheme, secret keys are placed in sensor nodes before deployment. When the nodes are deployed over the target area, the secret keys are used to create the network.

2.5 *Implementation of Pre-shared key Protocol*

<u>Step1</u>:Key setup phase:-

a)Generate key pool and corresponding key identifiers

b) Randomly select keys from key pool.

c) Load key into nodes memory

d) Save key identifiers of a keys and associated node identifier on controller

<u>Step2</u>: Shared-key discovery:-

a) Deployement of wireless sensor network

b) After deployment of WSN each node discovers its neighbor in communication range with which it shares key.

c) Nodes exchanges ids of key they possess and in this way they discover common key.

<u>Step3:</u>Path establishment:-

a) During the path key establishment phase path keys are assigned to selected pairs of sensors that are within communication range but do not share key

b) Node may broadcast the message with its key id, id of intended node and some key that it posses but not currently uses ,to all nodes with which it currently has established link. Those nodes rebroadcast the message to their neighbours

C) Once this message reaches the intended node, this node contacts the initiator of path key establishment.

2.6 *Simulation of key Management Scheme*

(i)Wireless Sensor Implementation:

The simulation is carried out using the Network simulator(version 2.35),which simulates the events such as sending, receiving, dropping, forwarding, etc. The wireless channel is used as the sensor nodes deployed communicate wirelessly with each other. The propagation models are used to compute the received power. When a packet is received, the propagation model determines the attenuation between transmitter and receiver and computes the received signal strength. The two-Ray ground Radio propagation model is used. An omni-directional antenna is employed for carrying out the transmissions which can transmit signal over a 360 degree angle. Omni-directional wireless sensor networks are modeled such that a bidirectional link is established between neighboring sensor nodes if they are within communication radius. [10]

The scenario is simulated for 150 seconds. The participating nodes are not stationary. The routing protocol which monitors and carries out the transmission is Ad-hoc On Demand Distance Vector routing Protocol(AODV).The following table gives an overview of all the simulation parameters used.

Simulator	NS-2.35
Channel Type	Wireless Channel
Mobility Model	Two-Ray ground Radio Propagation Model
Network Interface Type	Wireless Phy/IEEE 802.15.4
Antenna Model	Omni-directional
Number of mobile-nodes	10-100
Routing Protocol	AODV
Simulation Time	150 sec
Network Size(m*m)	1000 *1000
Packet Size	1024 bits

Table3 Simulation Parameters

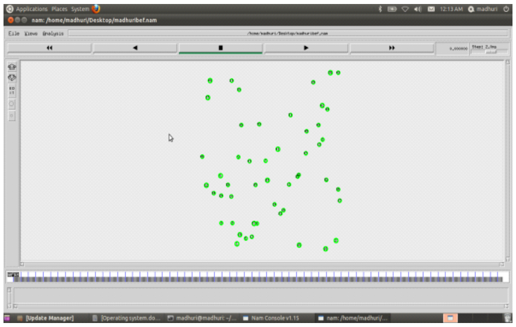

Fig 2.6.1Network Deployement

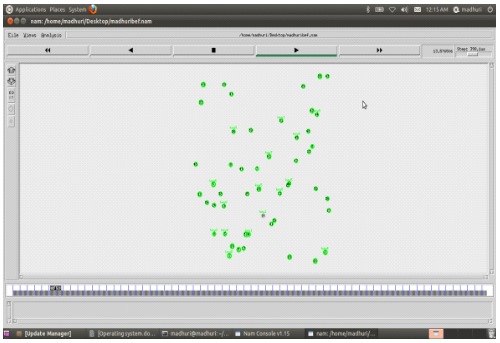

Fig 2.6.2 Key Generation

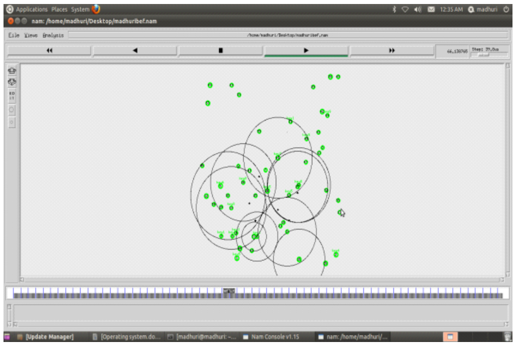

Fig2.6.3Nodes Within transmission range of each other

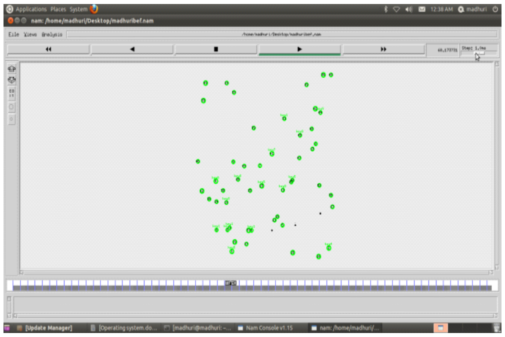

Fig 2.6.4 Nodes starts communication

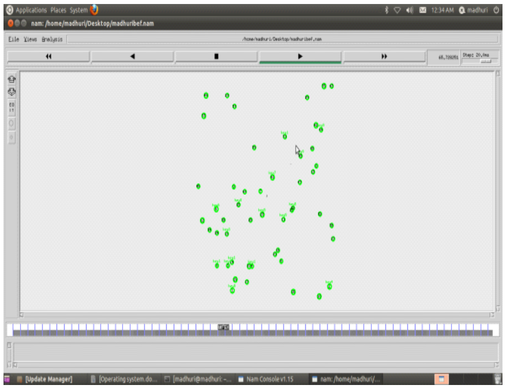

Fig 2.6.5 Nodes With Similar Keys Are communicating

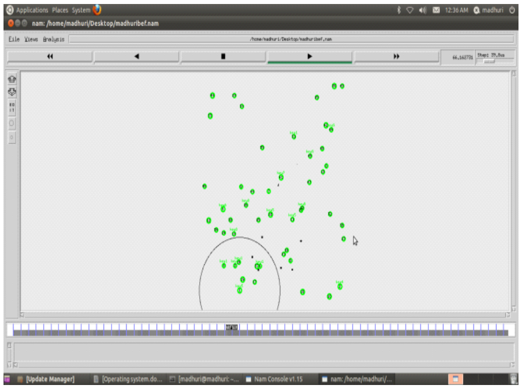

Fig 2.6.6 Packets Drop In Case Of Key Mismatch

3.Results

The following graphs were obtained after the implementation of PSK algorithm.

3.1 *Send Packets*

The first graph shows that there is a steady increase of request sent to the other nodes starting from default source to the destination. It can be seen from the graph that with the passage of time, the rate of packets send also increases as the normal behavior of the network. Since more and more nodes start communicating and sending request to each other. At this stage of sending HELLO message, which confirms that request has been sent to the nodes and they want to communicate with each others.

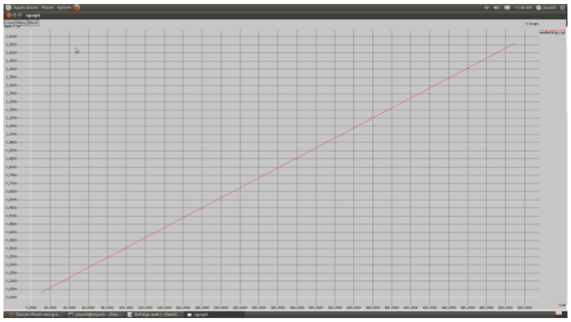

Fig3.1Packet Send Graph for PSK Scheme

3.2 *Receive Packets*

It's apparent from the graph that as the packets are sent, they are received but there is a sudden drop as the simulation proceeds. This means that at this stage the Key Pre-Distribution scheme works.There is disclosure of secrecy of key management. Key distributed at compile time in this scheme. But due to some resilience, there is a sudden drop of packets in the network. In other words, there is an implementation of uncommon sets. This is attributed to the fact that inspite of nodes being in the same range and having minimum cost of route as well as have established message routing protocol cycle complete, it suddenly shows drop in receiving data .As the key pairs seem to be not matching with each other and therefore they do not receive data and there's a dip. Although with the passage of time there's always an increase in peaks and valleys. In the graph the packets received are shown by the peaks graphs and the packets dropped are shown by the valleys.

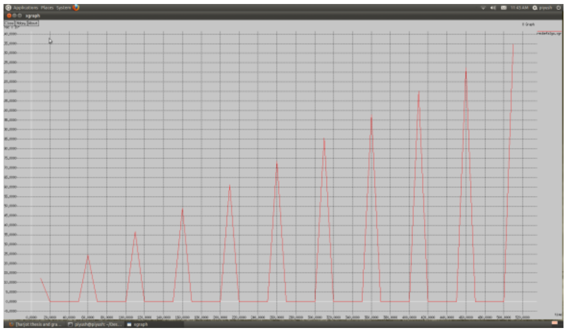

Fig 3.2 Received Packets for PSK Scheme

The graph illustrates that it has high computational overhead which is not too much suitable for WSN due to the effect of resilience and require more memory for storage of keys as well as exchange of keys for the simulation.

3.3 *Drop Packets*

This drop graph analysis wholly depends upon the send and receive graphs and its associated data.. Mathematically, drop is the difference between packets which are sent and received during a time span. As seen from the graph that with the passage of time if the packets are being received normally then there's a steady increase in the straight line but the packets are dropped, it shows a dip in the graph, the drop here (PSK) is due to large number of preconfigured keys which are random in nature and may not lead to a common set of key pairs which would have ensured the connectivity. It is apparent from the graph when the communication starts, as the

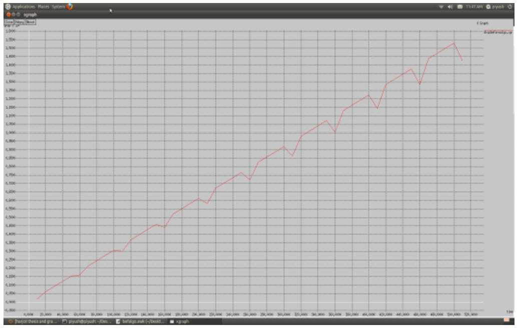

Fig 3.3 Drop Packets for PSK Scheme

Keys are exchanged when two nodes as per the protocol can communicate as their keys are disjoint in nature. So, as more and more communication occurs , after some steady increase there is a dip. The graph also explains that the packet delivery ratio has not proper connectivity with respect to scheme known as PSK. The probability against number of keys required are not proper which reducing the probability of connectivity.

3.4Energy Graph

It is apparent from the graph that as there is disclosure of secrecy of key in the PSK scheme, so there is occurence of fluctuation of energy pattern for different distinct of time. In other words, due to some limitation of PSK scheme the rate of energy pattern may varies for different interval of time which is shown in the graph below. The below graph does not clearly demonstrate the energy pattern which is somehow limitation for PSK (Pre Shared / Pre loaded) Key distribution.

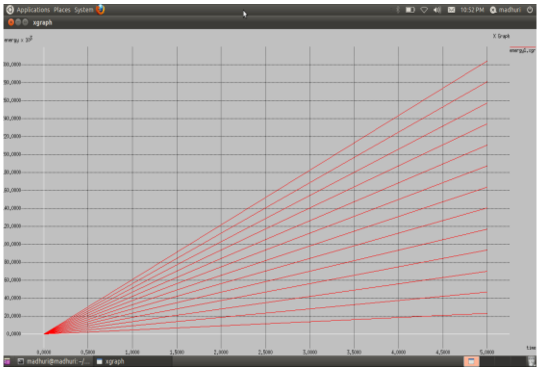

Fig3.4 Energy Pattern for PSK Scheme

4 Conclusion

Typically in Pre-Shared Key type of schemes, there is a major drawback related to its ***distribution property*.** Due to very large number of disjoint sets which get allocated due to random pre configured keys. The key connectivity in the whole network becomes a chance to establish link, sometimes even if the two nodes are close to each other in terms of their transmission and their receiving power they are unable to communicate. They unable to explain the energy consumption as the key scheme changes since each scheme effects the packet delivery ratio of network itself. Most of these paper are not demonstrating the impact of key schemes with respect to energy.

5. Future work

As we concluded there is a major drawback related to its ***distribution property*** in PSK.Because of which there is lack of key connectivity and energy .so much more work can be done to improve distribution property in pre-shared key scheme so that it improves key connectivity WSN and make it energyefficient.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *"Wireless sensor networks: a survey,"* in Computer Networks. vol. 38, 2002, pp. 393-422.

[2]http://www.worldscibooks.com/compsci/6288.html, *"Information Processing and routing in Wireless Sensor Networks "*© World Scientific Publishing Co. Pte. Ltd.[3] Muhammad,S., et.al.*"*

[3]*A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks"*, Department of Computer Engineering Kyung Hee University (Global Campus), Korea.

[4] WenliangDu,et.*al "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledg."*. Department of Electrical Engineering and Computer Science Syracuse University, Syracuse, NY 13244-1240, USA Email: {wedu, jdeng01, varshney}@ecs.syr.edu

[5] MokhtarAboelaze, FadiAloul, *"Current and Future Trends in Sensor Networks: A Survey",2005 IEEE.*

[6] Mohamed F. Younis, Senior Member, IEEE, KajaldeepGhumman, and Mohamed Eltoweissy, Senior Member, IEEE. *"Location-Aware Combinatorial Key Management Scheme forClustered Sensor Networks"* .

[7] Chiara Buratti ,et.al. *"An Overview on Wireless Sensor Networks Technology and Evolution"* ,WiLAB, DEIS at University of Bologna, Bologna, Italy.

[8] JiHeon Kwon, *"Improved Connectivity Using Hybrid Uni/Omni-directional Antennas In Sensor Networks"*, Department of Electrical and Computer Engineering Texas A&M University.

[9]http://blog.millennialnet.com/2011/06/30/good-wireless-sensor-network/, *"Good Wireless Sensor Network".*

[10] Dressler, F.*"A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks.Elsevier Computer Communications"* , vol. 31 (13), pp. 3018-3029, (2008).

[11]ElianaStavron ,*"Wireless Sensor Network limitations"*,http://webhosting.devshed.com/c/a/Web-Hosting-Articles/Wireless-Sensor-Networks-part-2-Limitations/.

[12] G. GELETA, “Performance Evaluation of Wireless Sensor Network Routing Protocols for Critical Condition Monitoring Applications,” Department of Computer Engineering, Addis Ababa University, Oct, 2007.

[13] J.Yick, B.Mukherjee and D. Ghosal, “Wireless sensor network survey,” Department of Computer Science, University of California, Davis, U.S.A, April, 2008.

[14] C. Haigaug, W. Huafeng, H. Jinchu and G. Chuanshan, “Event-based Trust Framework Model in Wireless Sensor Networks,” In the proceedings of the IEEE International Conference on Networking , Architecture and storage,June. 2008, pp. 359-364.

[15] G. Sklyarenko, “AODV Routing Protocol,” Institute for Informatic, Freie University Berlin, Berlin, Germany.

[16] SubhankarChattopadhyay,et.al., *"Key Pre-distribution and Key Revocation in Wireless Sensor Networks"*, Department of Computer Science and Engineering National

Institute of Technology Rourkela Rourkela, Orissa, 769 008, India May 2011.

[17] Laurent Eschenauer and Virgil D. Gligor.A key-management scheme for distributed sensor networks. In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 41- 47, New York, NY, USA, 2002. ACM.

[18] NS-2, the ns Manual (formally known as NS Documentation) available at http://www. isi.edu/nsnam/ns/doc.

[19]Ubuntu Operating System ,http://www.paulcolmer.co.za/index_ files/page0006.htm.

[20] Noor J. Ottallah, "Implementation of Secure Key Management Techniques in Wireless Sensor Networks" , B.S University of New Orleans, May, 2008.