Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Routing in Wireless Sensor Networks: A Review

Surabhi Singh
CSE, Amity University
India

Shilpi Sharma
CSE, Amity University
India

Suruchi Singh
E&T, MIT College of Engg.
India

Abstract- To protect the data in wireless sensor networks we require protocols that will make data transmission more secure from the attackers or intruders. In the past years we have seen that routing and transmission of data is not secure so we proposed certain technique and protocols to route data securely. A secure clustering protocol that achieves the desired security goals while keeping an acceptable level of energy consumption is a problem in wireless sensor network. In this paper we presented certain protocols and approach to make WSN more secure from attackers .Protocols that provide high level security ,authenticity, maintains network wide energy equivalence, prolongs network lifetime and provide all network security goals to protect the data that gives a better routing efficiency and data delivery.

Index Terms- Wireless Sensor Networks(WSN), Sensor Nodes, SPIN, Clustering, Encryption, Authentication, Compromised node, Attackers, Malicious nodes, attacks, security issues, path hopping, DBPH, LEACH, TTSF, BEARP

I. INTRODUCTION

A Wireless Sensor Network consist of sensor nodes that can sense, compute and communicate that enables a user to react in a particular environment. Sensor nodes are very small micro or tiny size nodes that measure or sense the surrounding conditions. These nodes measure the environmental conditions and send the data for further processing. This data can give us idea about the temp-erature, all kinds of weather and can also predict the future conditions. These wireless sensors are made up of nodes that has the ability to sense the information or facts which can be very useful for data collection and prediction. Sensor nodes are wireless that call for a major advantage that is no communication expense. They require no wiring set up that also benefits us by reducing man power. They are long lasting and tough due to which they can bear sudden temperature changes. These wireless nodes have the capability to communicate with other sensing nodes present in the network, infact they can process information in large amount. They are not very expensive or you can say they are economical and come in budget. We can use it for many purposes like in home applications, in laboratories etc. Economy means that we perform computations ,observation, sensing facts in budget that will not increase our expense so wireless nodes is the answer for this reason. Prediction of future is also done by them on the basis of data they collect from environment can also predict coming future. Sometimes scientist also tell us about the information that what is going to happen in next coming Decades which is given by wireless sensor nodes. Now we will study about various features and practical uses of wireless sensors.

Sensor nodes observe, sense and measure the environment temperature by capturing the facts or data that we cannot feel .Wireless Sensor Nodes communicate with other nodes present in their environment and pass on the information for further processing. This shows they can not only monitor but also have great communication power that benefits a lot. They are not costly and are very small in size. They consume very less amount of energy by radio ranges which is the main reason that cost overheads are very less. They perform monitoring or sensing in limits according to their capacity.

Self organized wireless nodes can also control activities happening in their surrounding and collect information that is preprocessed and can be used to display on internet. We can also trust them as the information they send are good and authentic, no duplicacy or virus infected messages in the data. These nodes are present in large number in the system of network and fastly collect facts that are used by us through internet.

We now discuss about the inside of wireless sensors that what it is made up of. The very first requirement to build nodes is a battery. It requires a small size battery that is inserted in sensor nodes which actually control the working of these wireless sensors. Infact bandwidth of nodes is very less or you can say minimum. It requires no maintenance cost because no replacement of battery is needed, so we can say they are highly economical.

All nodes sense the information not only form one side but they are bi directional and connection is depend entirely on power level and fading. Now we will study how these nodes exchange information among themselves. We all know that they communicate with each other to pass the information for the useful data extraction. They first collect the data from all the sensor nodes and aggregate them according to the level.

After the clusters are formed they are sent for processing. Nodes only pass the data and do not process it as it will increase the lifetime of network system. Transceivers are used for communication between the nodes. In short they are

very intelligent system and proved an advantage to the upcoming technology. The next generation of human man kind needs wireless technology to save man power and get extracted information in less time and wireless technology proved it.

II. PRACTICAL USE

Wireless sensors have various applications. These days we use them everywhere such as in home applications, schools ,colleges, bigger organizations etc. So we now discuss some practical uses of the wireless nodes. How it helps the nation ,firstly it can be used to spy criminals for close information. All CCTV cameras are fitted with these sensor nodes that collect and senses the activity of criminal that is controlled through a computer system which helps us to arrest the criminal gang.

It also helps in observing traffic of vehicles mainly on highways because large number of trucks travel via highway to transfer goods. They also check and monitor pollution level. How much level of dust and poisonous gases are increasing day by day in air and also measures noise level since the vehicular traffic is increasing so noise is also gradually changing and resulting in a higher level. They also check and quality of water ,how much purity is present.

Discovery channel has proved that use of this wireless technology is so good that we use GPS system to sense the behavior of animals. Special kind of GPS belts that contain sensor nodes are tied around the neck of animals to study the behavior of animals. GPS system consists of wireless sensor nodes that tells us about the behavior of animals.that is why we come to know how animals behave and react to events.

Perform processing of network to convert data (raw) into useful information Use of large number of sensor nodes around the island that forward data to satellite in order to provide data on internet.

To check composition of soil that how much percent organic matter etc is present is done through these nodes, to Check and monitor human heart rate , for the purpose of military and national security. It is used everywhere in every field and a unique watch is made using the sensor nodes that can be used to recognize the accident,how it happened ,at what time, weather, temperature etc. These sensor nodes can also be use to detect flood. Before the happening of flood it will be detected. It can also be used for agriculture purposes to measure the temperature so that we can estimate how to treat plants according to their temperature. It can be used in detection of car theft and surveillance of battlefield.

III. ROUTING PROTOCOL

Efficient and Secure Routing Protocols for WSN are as follows:-

3.1 DETECTION BASED PATH HOPPING (DBPH)

In Wireless Sensor Networks (WSN) various security approaches are proposed in order to make WSN more secure. This approach will work on the authentication as well as path hopping in order to provide security. Detection based Path Hopping technique is a method for making WSN more secure. It works in three phases:Selection of master node,Detection process and Data transmission

Following steps are followed in the Detection based path hopping technique:

- In this approach we will select number nodes we want to deploy. As the WSN are densely deployed so the number sensor nodes will large.
- After the deployment, the nodes, in the first phase we will select a sender called “MASTER NODE” which will be considered an authenticated node from the network.
- Second phase of the method is detection. In this node (MN) will then send authentication detection message. For authentication, key method used has a single key is distributed all over the network.
- All the nodes will reply to the authentication detection message . In the authentication reply they will send their network id and a network key to master node.
- After all reply received the master node; it will make a data base of authenticated or good nodes and unauthenticated or malicious nodes.
- The next step after selecting the sender and receiver is data transmission phase. In this phase data transmission will take place between node.
- In the data transmission the sender will first compute the nearest node to
  it using the formula in direction of receiver. This distance will be calculated by the sender by a formula called ”**DISTANCE FORMULA**”.
  √(x2-x1)^2 – (y2-y1)^2

3.2 BASED ON ENCRYPTION AND AUTHENTICATION ROUTING PROTOCOL (BEARP):

This protector consist of following stages:

- Near phase
- Protecting phase

Some secular characteristics are as follows**:**

- Data will be confidential
- Genuine data
- No alteration
- Original data

It contains following stages:

- Near phase
- Protecting phase

Near Phase

Near phase starts just after repurpose of sensing node. This can be done any time in the life of sensing node. This reconstruction can be done when Base Station request for it.

Protecting Phase

This piece of work is break into three act of works:

- Enquiry in data set or facts
- Selection of path to which data will be send
- Finally the facts/data will be routed or send

3.3 SENSOR PROTOCOL FOR INFORMATION via NEGOTIATION (SPIN)

This protocol has removed various problems of previous techniques/protocols by using negotiated data, communication of nodes among themselves about which data or facts they already contain and
what amount of data or facts they still want.
There are four kinds of subdivision**:**

- EC
- BC
- RL
- PP

SPIN-PP consists of **three types of messages**:

- ADV- it is used for advertising the presence of new facts/data
- Requesting new facts/data-REQ
- Facts that we have to route/send

The procedure for implementing the protocol will be as follows:
1.)Presence of CA(main) in network/system
2.)Presence of second level CA in system/network
3.)Second level CA contains information about its group nodes.
4.) Authenticity of every node of the group will be checked by its own private/personal key.
5.) 2^32 number of IP addresses are available, that we have assumed and 231 total sensing nodes are present.
6.)It is compulsory that every sensing node should have 2 IP add to participate in communication. When node become part of system/network first IP add. is given to it and second IP add.by its CA(secondary) .

Beginning Phase

The nodes will search for CA(second) so that it will stick/attach to it. Then Internet Protocol(IP)
addresses were allocated to the nodes. Now the further steps are as follows:

- Nodes will send a find packet to all its secondary CA.
- The node will receive an acknowledgement from CA(secondary).
- After this has been done the sensor node will again send an acknowledgement packet to another nearest CA to it, and tell about its choice.

Create Phase

Once the beginning phase is over the the sensing node enters the system/network, it will then starts a create phase which consist of IP add allocation to sensor nodes that will then be used in communication process as multiple add.
It has algorithms as follows:
1.)Create phase of CA
2.)Secondary phase of CA
3.)Grouping phase

Communication Phase

After the beginning and create phase are over, every sensor node will run this algo to communicate with other nodes in the system/network.
1.)Every sensor node is sensing facts or data, busy in routing procedure or waiting for information (data).
2.)If a sensor node contain some data it will initially send that data and then accept new data.Algorithms that come under this phase are as follows:

- Receiving of data
- Sending of data

3.4 LOW ENERGY ADAPTIVE CLUSTER HIERARCHY(LEACH):

It is a cluster based protocol that equally distributes energy in network to sensor nodes. This protocol enables robustness and scalability to dynamic network. LEACH enables confidentiality and authenticity by using pairwise key between cluster head and their cluster members. In set up phase cluster head message contains MAC and ID that is shared only by base station and cluster head. The Base Station will then authorize the message send by cluster head. After that the Cluster Head ID will added to valid node list. BS will broadcast the valid nodes throughout the network. The nodes will then connected to authenticated CHs and broadcast confirm message for approved sensor nodes. Working of this protocol :

1.)Cluster Head and sensor nodes will communicate via pair wise key that has no communication cost or expense.
2.)CH and its nodes will then generate a joined request, which will be useful for further communication. In next phase the nodes will then send its ID and MAC add. to head of cluster.
3.)Cluster Head will send its child node ID in an encrypted message to the Base Station. It will also send Mac add. via shared keys.

- **THREE-TIER SECURITY FRAMEWORK (TTSF):**

TTSF protocol is proposed in order to deal with attack named as mobile sink replication. In this framework we select few wireless nodes that are stationary nodes and they can access data without movement. These nodes are authentic nodes that are present in network system that trigger the sensing nodes to aggregate their data to sink(mobile). The message that is requested by sink will then be sent via stationary access sensor nodes.

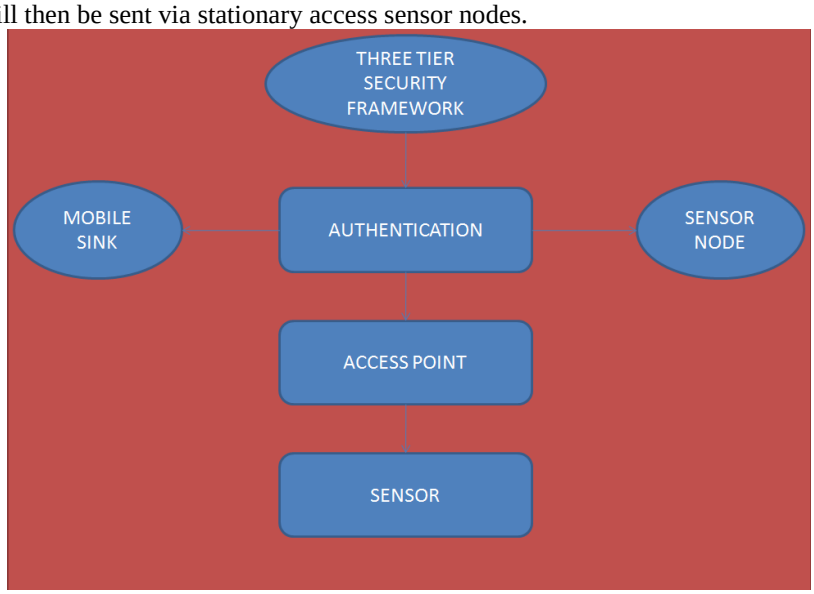

Fig.1 Three tier Security Framework

1.)Detection of compromised nodes: The wireless nodes are detected using mobile polynomial tools that can bears attack.
2.) Status bits are collected along with ID's: Here we collect the bits in which I representscompromised nodes and 0 represents the node that are normal.
3.) Now on the basis of threshold of bits we will take the decision of deploying new nodes in the network.
4.)Now we form the clusters of nodes that are mostely used for the life of the sensor network.

IV. CONCLUSION

We have studied various protocols to provide better security in wireless sensors and every protocol has its own security features and method to provide secure routing to WSN.

ACKNOWLEDGEMENT

I would like to express heartfelt gratitude towards my mentor Ms. Suruchi Singh and Ms. Shilpi Sharma for guidance and helping me in completing this work successfully.

REFRENCES

[1] Deng J, Han R and Mishra S: 'INSENS: *Intrusion-tolerant routing for wireless sensor networks*', Computer Communications, 29(2006), pp 216-230.
[2] Bing Wu, Jie Wu, Eduardo B. Fernandez, Mohammad Ilyas, Spyros Magliveras, *Secure and efficient key management in mobile ad hoc networks*, Journal of Network andComputer Applications, 30 (2007), 937-954.
[3] Ito, T. , Ohta, H. , Matsuda, N. , & Yoneda, T. . *A key predistribution scheme for secure sensor networks using probability density function of node deployment*. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, November 2005, pp. 69-75.
[4] S.Ganesh, DLRAmutha "*Network Security in Wireless Sensor Networks Using Triple Umpiring System*" European Journal of Scientific Research, 2011, VoL64, issue L

[5] Ganesh.S, DLRAmutha "*Modified Triple Umpiring System for Wireless Sensor Networks*" PSG tech-National Journal of Technology, Vol. 8, issue I, March 2012, pp 48-63.

[6] 1] I. F. Akyildiz, W. Su, Y. ankarasubramaniam, and E. Cayirci, "*A survey on sensor networks*," *IEEE Communications Magazine*, Vol. 40, Issue 8, pp. 102-114, August 2002.

[7] G. Pottie and W. Kaiser, "*Wireless Sensor Networks*",*Communications of the ACM*, Vol. 43, Issue 5, pp. 51–58, May 2000.

[8] W. Hu, V.N. Tran, N. Bulusu, C. Chou, S. Jha, A. Taylor, "*The design and evaluation of a hybrid sensor network for Cane-Toad monitoring*", in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, Los Angeles, CA, pp.382- 387, 2005.

[9] S. Hedetniemi, A. Liestman, ''*A Survey of Gossiping and Broadcasting in Communication Networks*,'' *IEEE Networks*, Vol. 18, No. 4, pp. 319–349, 1988.

[10] W.R. Heinzelman, J. Kulik, and H. Balakrishnan,"*Adaptive Protocols for Information Dissemination in Wireless Sensor Networks*", in *Proc. of 5th annual ACM/IEEE international conference on Mobile computing and networking*, Seattle, Washington, pp. 174-185, 1999.

[11] Babli Kumari, Jyoti Shukla "*Secure Routing in Wireless Sensor Network*" in International Journal of Advanced Research in Computer Science and Software Engineering :Volume 3, Issue 8, August 2013 ISSN: 2277 128X .

[12] S.Ganesh, S.Sankar, S.Saravanakumar, Mr.Sean Laurel Rex, Mr.M.Dinesh" *Three Tier Security Frame Work for Wireless Sensor Networks*" in Proceedings of the "International Conference on Advanced Nanomaterials & Emerging Engineering Technologies" (JCANMEET-20J3).

[13] Jiliang Zhou"*Efficient and secure Routing Protocol Based on Encryption and Authentication based on Wireless Sensor Networks*".

[14] Mona El_Saadawy, Eman Shaaban "*Enhancing S-LEACH Security for Wireless Sensor Networks*".

[15] Dhurandher, Sanjay K., Mohammad S.Obaidat, Gaurav Jain, Isha Mani Ganesh, and Vinay Shashidhar. "*An Efficient and Secure Routing Protocol for Wireless Sensor Networks Using Multicasting*", 2010 IEEE/ACM Int l Conference on Green Computing and Communications & Int l Conference on Cyber Physical and Social Computing, 2010.

[16] Lei Kong. "*Time Synchronization algorithm based on Cluster for WSN*", 2010 2nd IEEE International Conference on Information Management and Engineering, 04/2010.

Table I : Comparison of various Protocols:

ROUTING PROTOCOL	**CLASSIFICATION**	**POWER CONSUMPTION**	**AGGREGATION OF DATA**	**SCALABILITY**	**QUERY BASED**	**OVER HEAD**	**DATA DELIVERY MODEL**	**QoS**
LEACH	Hierarchical	high	yes	yes	no	high	Cluster head	no
TTSF	Hierarchical	highest	no	yes	no	low	Chain based	no
SPIN	Data centric	limited	yes	yes	yes	low	Event driven(flow determined by events)	no
Directed Diffusion (DD)	Data centric	limited	yes	no	yes	low	Demand driven(depends on consumers demand)	no
BEARP	hierarchical	high	no	yes	no	high	Cluster head	no

