Volume 3, Issue 8, August 2013 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 Network

Babli Kumari, Jyoti Shukla
CS&E Deptt, Amity University
India

Abstract: Advances in the electrical and electronics communication technologies led to large scale development and research in area of Wireless Sensor Network. Wireless Sensor network have numerous applications in recent scenarios. WSN have a large number of constrained attached to them such as less processing capability, low memory, limited energy resources and security issues. WSN generally deployed in natural environment hence a large number of security issues are there. In order to protect the data in WSN we require approaches that will make data transmission more secure from the attackers. In this paper we presented an approach called Detection based path hopping to make WSN more secure from intruders and attacks.

Keywords: Wireless Sensors Networks, Attackers, Malicious nodes, attacks, security issues, path hopping.

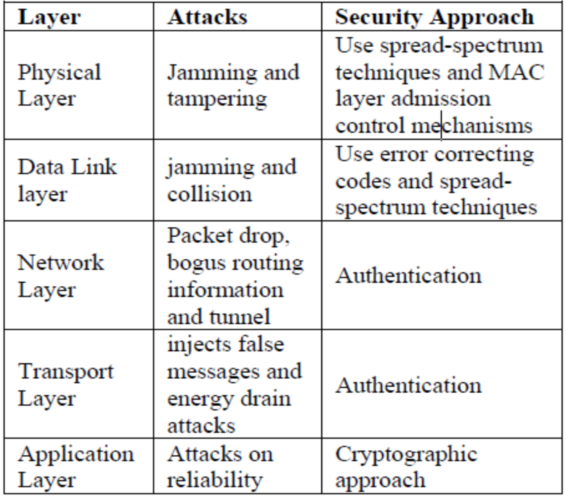
I. Introduction

Wireless Sensor Networks are densely deployed low cost, low processing power, less memory and limited energy resource networks. In recent years WSN found a large number of applications in the field of both research and academics. In WSN, the nodes are called sensors which sense the data like temperature, humidity, noise or sound, pressure soil variety, movements of objects, stress levels, detection of objects around and other properties from the surrounding and send this information to the base station for further analysis and decision making. WSN are mainly deployed in natural environment where the sensor nodes remain unattended and used for surveillance and monitoring. WSN finds a large application in the fields like military, traffic control, home automation, healthcare applications and many civilian application areas. Since WSN sensor nodes are deployed in unattended and rough natural environment there are large number of security issues with them. Data transmitted in WSN should be safeguarded from unauthenticated and unauthorized nodes and attackers. We have to maintain the authenticity, integrity and confidentiality of the data that is transmitted between the nodes of the network. Intruder may attack the network in many ways as tampering and jamming the data packets affect the integrity, unauthorized access to the network (Eavesdropping), pretending to be authenticated node to capture the data.

There are many routing protocols for maintaining and management of WSN. Different categories of routing protocols are flat-based, Hierarchical, location-based, Network flow and QoS, Mobility-based, Multipath-based, Heterogeneity-based protocols. The above mentioned category deals with maintenances and management routing information, making the network to live longer by lowering the energy consumption (energy efficient) and maintain network infrastructure. All the protocols lacks in providing proper security mechanism for Wireless Sensor network.

There is no proper layered standard for Wireless Sensor Networks. Here is a summarized view of possible attacks and their security solutions.

Table 1: Layer based attacks and possible security approaches.



Layer	Attacks	Security Approach
Physical Layer	Jamming and tampering	Use spread-spectrum techniques and MAC layer admission control mechanisms
Data Link layer	jamming and collision	Use error correcting codes and spread-spectrum techniques
Network Layer	Packet drop, bogus routing information and tunnel	Authentication
Transport Layer	injects false messages and energy drain attacks	Authentication
Application Layer	Attacks on reliability	Cryptographic approach

These are some of the approaches to make sensor networks secure from attackers and malicious nodes in the networks that will harm the integrity and confidentiality of the transmitted data.

II. Literature Review

WSN have a number of security issues related to failure and intruder. Due to deployment of nodes in unattended environment WSN network prone to various security attacks. From previous research and study a large number of security threats are enumerated in WSN. These attacks disrupt the integrity, confidentiality and authenticity of the transmitted data. The intruder may gain unauthorized access to data packets, modify the original data, inject false messages, may imitate as an authenticate sensor node. Some of the most common security threats in WSN are:

- Sink hole attack
- Wormhole attack
- Selective forward attack
- Sybil attacks
- Sniffing attacks
- HELLO flood attack
- Spoofed, altered, or replayed routing attack
- Energy drain attack
- Black hole attack
- Node replication attack
- Acknowledgement attacks
- Denial of service
- Attacks on information transit

Most of the routing protocols like location based, flat based, hierarchical, and Network flow and QoS protocols are very much prone the attacks enumerated above. Protocols like hierarchal are prone to almost all the threats described. Hence the protocols till used in WSN only concern with the data transmission and routing the information. These protocols lack in providing a secure data transmission. So in order to provide WSN a more secured and reliable data transmission we have to provide good security mechanisms. Many security approaches are proposed, some of them are key distribution method, spread spectrum, authentication techniques. List of some techniques are:

- Unique pair wise keys
- Encryption
- Monitoring
- Error correcting code
- Key management schemes
- Random key re-distribution
- Radio resource testing
- Bidirectional Verification
- Multi-path multi-base station routing
- Adaptive antennas
- Two way authentication
- Three way handshake

The above mention security techniques are used certain to a particular security attacks like the three way handshake technique is a defense approach against HELLO flood attack, similarly radio resource testing is used against Sybil attack and so on. Here in this paper we proposed a defense technique called "Detection based path hopping" for better security in WSN. This approach will maintain the integrity and confidentiality of the data transmitted. This approach is a combination of authentication of node and path hopping technique. The approach is discussed below.

III. Detection Based Path Hopping Technique

In Wireless Sensor Networks (WSN) various security approaches are purposed in order to make WSN more secure. In this paper we introduce a security mechanism which 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 Wireless Sensor Network more secure. Detection based path hopping Technique works in three phases:

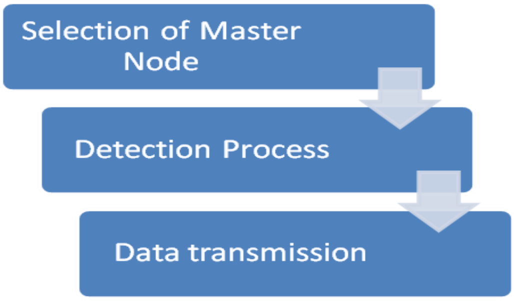


Figure 1: Steps of Detection based path hopping

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

1. 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.
2. After the deployment the nodes, in the first phase we will select a sender called **"Master Node"** which will be consider an authenticated node from the network.
3. Second phase of the method is detection. In this master node (MN) will then send authentication detection message to all the nodes in the network. For authentication network key method is used where a single key is distributed all over the network.
4. 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.
5. After all reply received the master node; it will make a database of authenticated or good nodes and unauthenticated or malicious nodes.
6. The next step after selecting the sender and receiver is data transmission phase. In this phase data transmission will take place between nodes.
7. In the data transmission the sender will first calculate the shortest path to the neighbor in the direction to the receiver. This distance will be calculated by the sender by a formula called "**distance formula**". Distance vector is method to calculate distance between two points in two dimension plane. Let suppose there are two points p1 and p2 having coordinates (x1, y1) and (x2, y2) respectively. The distance formula to calculate the distance between two points' p1 and p2 will as follows:

$$\textbf{Distance (d)} = \sqrt{(x2-x1)\hat{}2 - (y2-y1)\hat{}2}$$

Where d is the distance between p1 and p2.

This value of d will decide the next intermediate in the path.

8. After the selection of the shortest path to next node the sender node will check whether the node with shortest path is an authenticated node or malicious node.
9. If the node with shortest path is an authenticated node then the sender will send data to that node otherwise if next node is a malicious node than the sender will check node with less distance and same procedure will be performed until an authenticated node will not be found. As soon as authenticated node will be found the sender will be sending data to that node. This procedure is also called path hopping.

IV. Simulation

Simulation of the approach in done on MATLAB. Here in step by step presentation of the Pre-Detection Approach simulation on MATLAB. In the figure 2 it shows node deployment where the user will enter the number of sensor nodes to be deployed. In the scenario the sensor nodes are represented by blue colour.

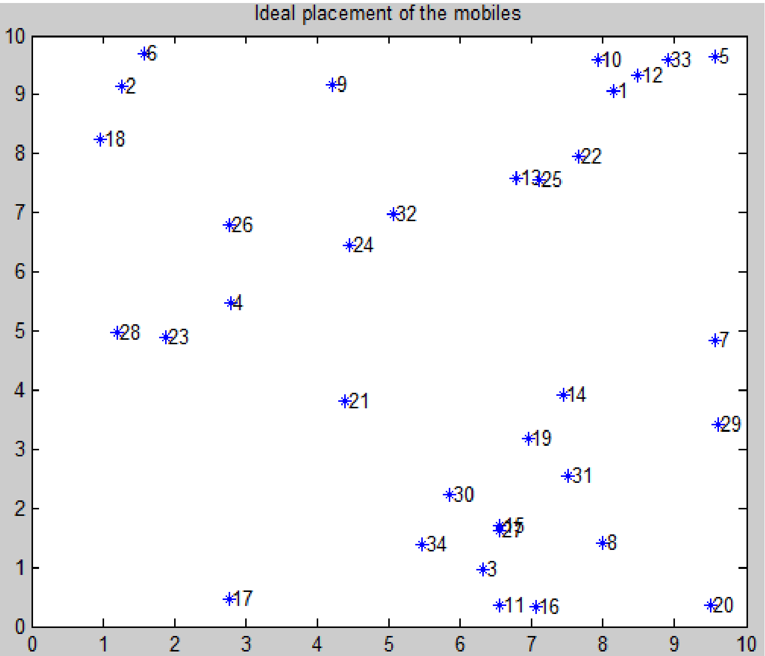


Figure 2: Node deployment

In the simulation shown below (figure 3) after nodes are deployed now we select sender and receiver node, the sender node will become Master Node and will send request for authentication to each node.

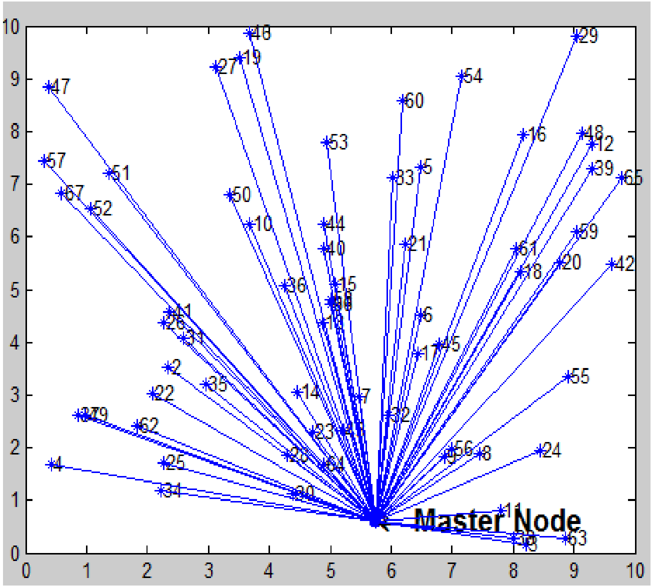


Figure 3: Node Detection by Master Node

In the figure 4 after detection process the nodes are categorized into two categories named as authenticated and malicious nodes. The malicious nodes are represented in the simulation by colours like red, green, dark blue colours and authentication nodes are represented by blue colour. The sender or Master Node will make a data base of malicious nodes and authentication nodes. This data base will help out on finding path between receiver and sender which will be free from malicious node.

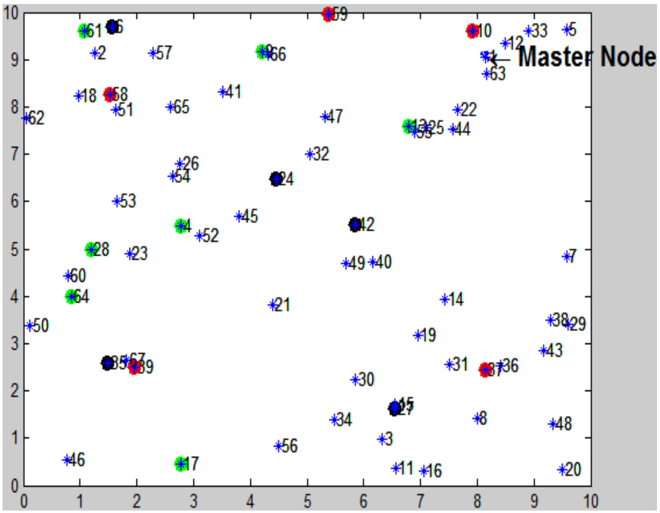


Figure 4: Detection of Malicious Node

In figure 5 path hopping techniques is simulated where data transfer from faulty nodes but from different routes to the receiver.

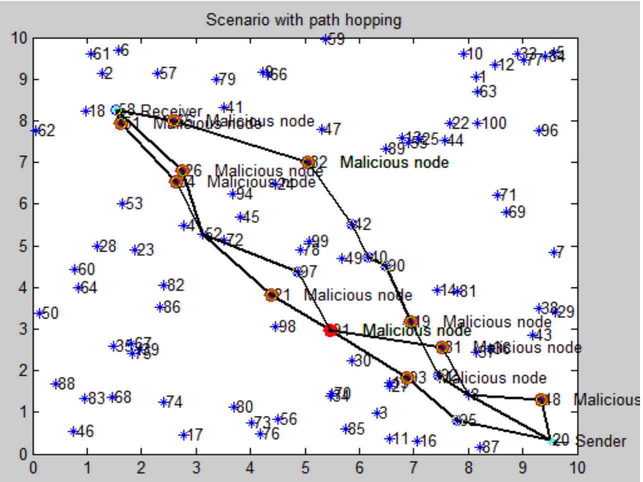


Figure 5: Path hopping in the Network

In the next simulation (figure 5) data transmission is taking place. The sender first selects the node with least distance in the direction of the receiver and if the selected node is malicious node than it will select other node with second least distance from the receiver. Similarly this process will work on all the intermediate nodes until the next receiving node.

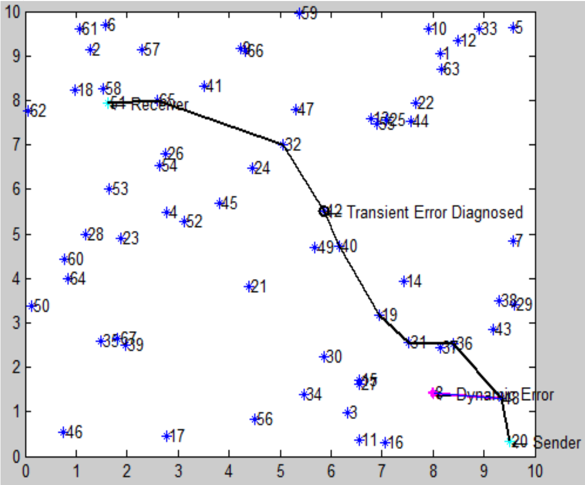


Figure 6: Data transmission

This approach will reduces threat to data integrity and confidentiality from attackers and malicious nodes. The detection and path hopping will make the data transmission more secure as compared to other techniques in WSN. The data transmission in the Pre-Detection approach will more secure than other security approach as it include authentication for sinkhole like attacks and path hopping for spoofing, altered and replayed attacks. Hence increase the data delivery ratio and reduces packet loss in the network.

V. Results

In the simulation there are three scenarios are considered: one is simulation without error, second simulation with error and last is simulation with Detection based path hopping method. The comparisons are made on two parameters 1. Delay in routing 2. Energy loss and 3. Packet loss. The first figure shows the delay in routing in error free simulation, with error simulation, path hopping and detection with path hopping.

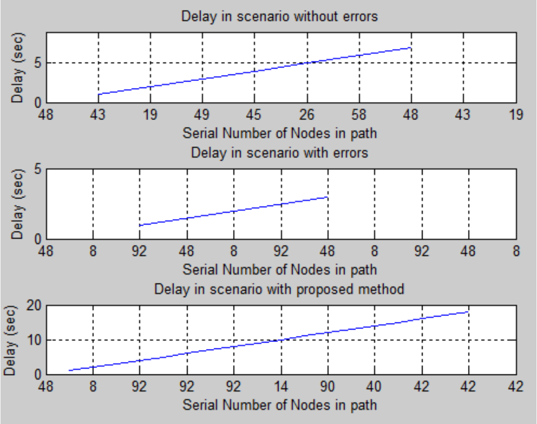


Figure 7: Delay comparison

Figure below shows the comparison between energy loss in simulation with error and without error and Detection based path hopping. This shows that due to error data transmission is stopped. Energy loss comparison in three simulations.

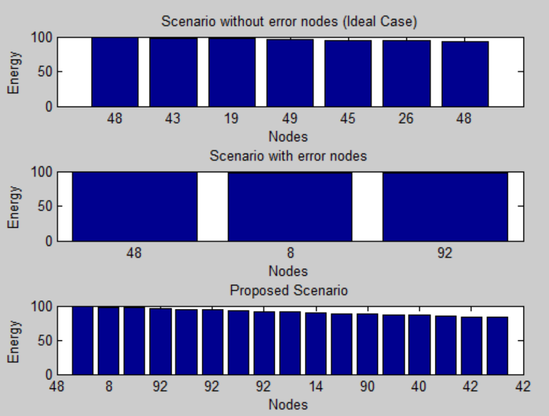


Figure 8: Energy Loss

The figure 9 shows the packet loss in original path hopping and detection based path hopping. Packet loss in original path hopping is less than Detection based path hopping.

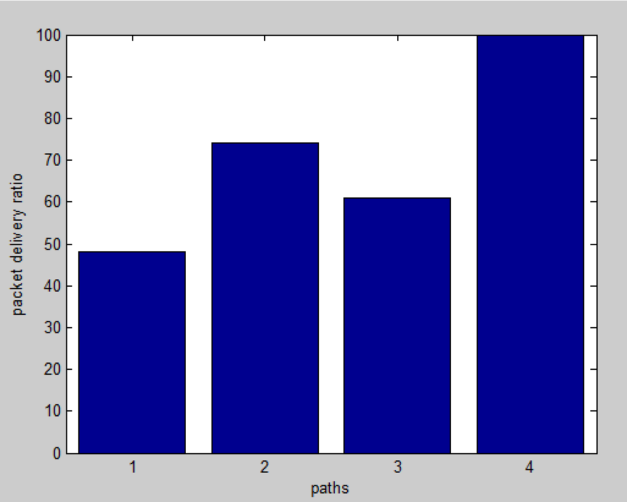


Figure 9: Packet loss in Path hopping and Detection based path hopping.

VI. Conclusion

Security is one of the major concerns in Wireless Sensor Networks because of the network deployment. Intruder can attack the network in many ways, it could be physical or by gaining access to authenticated node. A large number of security mechanisms are purposed in Wireless Sensor Network out of which one is path hopping technique. In the thesis enhanced the security of path hopping with adding detection method. We simulated the environment in various situations that is network with error, without error, path hopping, with detection based path hopping technique. With the results we have seen that the packet delivery ratio of the original path hopping technique is less than the packet delivery ratio in detection based path hopping technique.

Hence, it secures the network more than the existing path hopping technique.

VII. Future Scope

Since in Wireless Sensor Network there is a tradeoff between energy and security so there can be enhancement for the energy efficiency of the technique. Here only simulation of the technique is done; work can be done on combining this technique with any routing protocol in Wireless Sensor Network and practical implementation of the technique.

References

[1] Culler, D.E and Hong, W., “Wireless Sensor Network”, Communication of the ACM, Vol.47, No. 6, June 2004, pp.30-33.

[2] Akyildiz, I. F., Su , W., Sankarasubramaniam, Y, and Cayirci, E., “Wireless Sensor Networks: A Survey”, Computer Networks, 38, 2002, pp. 393-422.

[3] Chonggun kim, Elmurod Talipov, and Byoungchul Ahn, “A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks”, International Federation for Information processing, 2006, pp. 522-531.

[4] Kemal Akkaya and Mohamed Younis, “ A Survey on routing protocols for wireless sensor networks”, Elsevier,2003.

[5] CHEE-YEE and SRIKANTA P. KUMAR, “Sensor Networks: Evolution, Opportunities, and challenges”, Proceeding of the IEEE, Vol.91, No.8, Aug 2003.

[6] Jan Steffan, Ludger, Mariano Cilla, Alejandro Buchmann, “Scoping in Wireless Sensor Networks”, ACM, 2004.

[7] Jyoti Shukla and Babli Kumari, “Security threats and Defense Approaches In Wireless Sensor Network: An Overview”, IJAIEM, Vol. 2, Issue 3,Mar 2013

[8] Shio Kumar Singh, M P Singh, and D K Singh, “ Routing Protocols in Wireless Sensor Networks- A Survey”, IJCSES, Vol .1, No. 2, Nov 2010.

[9] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, “ Security issued in Wireless Sensor Networks”, International journal Of Communications, Vol.2,Issue. 1,2008.

[10] Elmurod Talipov, Donxue Jin ,Jaeyoun Jung, Ilkhyu Ha, YoungJun Choi, and Chonggun Kim, “ Path Hopping Based Reverse AODV for Security”, Springer, pp. 574-577, 2006.

[11] A. Agah, S. K. Das , K. Basu, and M. Asadi. “Intrusion detection in Sensor Networks: a Non- Coorperative Game Approach”, IEEE, pp. 343-346,2004.

[12] C. Bekara and M. Laurent-Maknavicious. “ A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks”, IEEE, pp.59-59, 2007.

[13] C. Blundo, A.D.Santis, A. HerzBerg, S. Kutten, U. Vaccro, and M. Yung. “ Perfectly- Secure Key distribution For dynamic Confrences”, Information and Computation, pp. 1-23, 1998.

[14] R. Brooks, P.Y. Govindaraju, M.Pireretti, N. Vijaykrishnan, and M. T. Kandemir, “ On the Detection Of Clones in Sensor Networks Using Random Key Predistribution, IEEE,pp. 1246-1258,2007.