Secure Routing in Wireless Sensor Network

Renu Bala
Research Scholar
Department of Computer Science and Engineering
Ganga Institute Of Technology & Management, Kablana

Dr. Yashpal Singh
Associate Professor
Department of Computer Science and Engineering
Ganga Institute Of Technology & Management, Kablana

Abstract

Wireless Sensor Networks is the new concept in the field of networks consists of small, large number of sensing nodes which is having the sensing, computational and transmission power. Due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks. Moreover, routing protocols are designed, taking the consideration of power consumption not security as a goal. As security plays an important role in the ability to deploy and retrieve trustworthy data from a wireless sensor network. The proper operations of many WSNs rely on the knowledge of routing algorithms. However, most existing routing algorithms developed for WSNs are vulnerable to attacks in hostile environments. Current routing protocols assume the networks to be benevolent and cannot cope with misbehaviour of nodes. The misbehaviour may be due to node being malicious to save the battery power. Whenever any device comes within the frequency range can get the access to the transmitting data and may affect the transmission. Thus, this work has significant importance, to build a highly secure system through frequency hopping.

Keywords: Security, Wireless Sensor Networks, Frequency hopping

I. INTRODUCTION

Due to the recent advancement in micro-electro-mechanical systems (MEMS), wireless communication like Bluetooth, IEEE 802.11, or MANETs, a new concept of networking has emerged known as Wireless Sensor Networks (WSNs). Wireless Sensor Network, consists of large number of sensor nodes having the capability of wireless communication, limited computation and sensing. WSN was initially developed for military and disaster rescue purposes but because of the availability of ISM band (2.4 GHz), the technology is now emerging in public applications. The salient features in Wireless Sensor Network makes it different from other network; self-organize, low power, low memory, low bandwidth for communication, large-scale nodes, self-configurable, wireless, infrastructure-less. Therefore, WSN design must encounter these features in order to provide a reliable network. However each sensor node is equipped with its own sensor, processor and radio transceiver, so it has the ability of sensing, data processing and communicating with each other.

Wireless Sensor Networks (WSN) relies on collaborative work of large number of sensors. For this reason, they are deployed densely throughout the area where they monitor specific phenomena and communicate with each other and with one or more sink nodes that interact with a remote user. The user can inject commands into the sensor network via the sink to assign data collection; data processing and data transfer tasks to the sensors in order to receive the data sensed by the network. However, due to the lack of tamper- resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks.

WSN are prone to failure and malicious user attack because it is physically weak, a normal node is very easy to be captured to become a malicious node or by inserting a malicious node in the network. The malicious nodes try to disrupt the network operation by modifying, fabricating, or injecting extra packets; they may mislead operation of packet forwarding or will try to consume the resources of the nodes by making them believe that the packets are legitimate. The malicious node will not cooperate in the network operation resulting in the malfunction of the network operation. This happens because any device within the frequency range can get access to the data. So, we need a secure way to protect the network. Wireless communication only affects the physical, data link and network layers of the OSI layer.

II. LITERATURE REVIEW

In August 2000,Intanagonwiwat, R. Govindan, and D. Estrin, gives "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00).

In 2001, I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, describes the concept of sensor networks which has been made viable by the convergence of micro- electro-mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed.

In 2002, Anurag Dagar, Vinod Saroha, presents an efficient coverage scheme for wireless sensor networks. This scheme focuses on two coverage strategies of wireless sensor network which are compared on different parameters , where Delaunay triangulation is more efficient coverage strategy as compared to square grid deployment strategy because in Square grid coverage strategy if we increase the sensing area than overlapping of sensing area is increased which is not desirable for valid data in coverage of region of interest where as in Delaunay, if we increase the sensing range of sensors than each node can communicate with other nodes in the network.

In 2006 J. Zheng and Myung J. Lee gives A comprehensive performance study of IEEE 802.15.4 – Sensor Network Operations,which have given the best results in the field of sensor networks.

In 2010, Yunhao Liu, Senior Member, IEEE, Kebin Liu, and Mo Li, Member, IEEE, Network diagnosis, an essential research topic for traditional networking systems, has not received much attention for wireless sensor networks (WSNs). Existing sensor debugging tools like sympathy or EmStar rely heavily on an add-in protocol that generates and reports a large amount of status information from individual sensor nodes, introducing network overhead to the resource constrained and usually traffic-sensitive sensor network. We report our initial attempt at providing a lightweight network diagnosis mechanism for sensor networks. We further propose PAD, a probabilistic diagnosis approach for inferring the root causes of abnormal phenomena. PAD employs a packet marking scheme for efficiently constructing and dynamically maintaining the inference model. Our approach does not incur additional traffic overhead for collecting desired information. Instead, we introduce a probabilistic inference model that encodes internal dependencies among different network elements for online diagnosis of an operational sensor network system. Such a model is capable of additively reasoning root causes based on passively observed symptoms. We implement the PAD prototype in our sea monitoring sensor network test-bed. We also examine the efficiency and scalability of this design through extensive trace-driven simulations.

In 2010,Peter Corke, Fellow IEEE, Tim Wark, Member IEEE, Raja Jurdak, Member IEEE, Wen Hu, Member IEEE, Philip Valencia, Member IEEE, and Darren Moore, Member IEEE, concerned with the application of wireless sensor network (WSN) technology to long-duration and large-scale environmental monitoring. The Holy Grail is a system that can be deployed and operated by domain specialists not engineers, but this remains some distance into the future. We presen tour view sasto why this field has progressed less quickly than many envisaged it would over a decade ago. We use real examples taken from our own work in this field to illustrate the technological difficulties and challenges that are entailed in meeting end-user requirements for information gathering systems. Reliability and productivity are key con- cerns and influence the design choices for system hardware and software. We conclude with a discussion of long-term challenges for WSN technology in environmental monitoring and outline our vision of the future.

According to Uday B. Desai B. N. Jain S. N. Merchant , The area of WSN is thriving and every day new ideas are emerging. A strong testimony to this is the recent report on Smart Sensor Networks: Technologies and Applications for Green Growth, by OECD: Organization for Economic Cooperation and Development, Dec. 2009 [49]. This report contributed to the OECD Conference on "ICTs, the environment and climate change", Helsingør, Denmark, 27-28 May 2009, and is a contribution to the OECD work on Green Growth.

In 2012, Deepika Thakral, Neha Dureja, Wireless sensor networks are set to become a truly pervasive technology that will affect our daily lives in important ways. We cannot deploy such a critical technology, however, without first addressing the security and privacy research challenges to ensure that it does not turn against those whom it is meant to benefit. Other applications include climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion. WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge.

This paper studies the security problems of WSN based on its resource restricted design and deployment characteristics and the security requirements for designing a secure WSN. Also, this study documents the well known attacks at the different layers of WSN and some counter measures against those attacks. Finally, this paper discusses on some defensive measures of WSN giving focus on the key management, link layer and routing security.

III. PROBLEM DEFINITION

Most current WSN routing protocols assume that the wireless network in beginning and every node in the network strictly follow the routing behavior and is willing to forward packets for other nodes. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes are present in the network.

A commonly observed misbehavior is packet dropping. Practically, in a WSN, most devices have limited computing and battery power while packet forwarding consumes a lot of such resources. Thus some devices would not like to forward the packet for the benefit of others and they drop packets not destined to them. On the other hand, they still make use of other nodes to forward packets that they originate. These misbehaved or malicious nodes are very difficult to examine that whether the packet dropping is intentionally by malicious node or dropped due to link error. WSNs have many characteristics that make them very vulnerable to malicious attacks. These are:

A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.

Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.

Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. However, attackers can break weak security protocols easily.

IV. RESEARCH METHODOLOGY

This will show the result of simulation.The analysis is being done on the basis of the results of *.nam file and the *.tr file with the help of Network Animator (NAM) and tracegraph by plotting the 2D and 3D graphs. We also evaluate the performance of the protocol by using AWK programming. With the help of AWK programming we obtain the results in percentage. Simulation has been divided in four parts that are given below:

A. AODV Simulation

In the simulation of simple AODV, experiment is carried over 25 nodes. In the ns2-allinone package NAM is a build-in program. NAM helps us to see the flow of route request (RREQ) and route reply (RREP). It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. Figure 6.1 and figure 6.2 are animation capture of WSN with25 nodes. The source (node 10) is broadcasting RREQ message to all its neighbors and Node 1which is the destination node, is sending RREP (route reply) back to the source. The nodes with the same frequency will receive the message and forward it to its neighbor, while the nodes with different frequency will drop the packet. In figure 6.2, a packet of blue color is on transmission from the source (node 10) to the destination (1) Since there is peer-to-peer communication between source node (10) and destination node (1), so no packet will be dropped. In figure 6.3 tracegraph proves that dropped packets are zero. This high throughput is expected because all the nodes are using the same frequency.

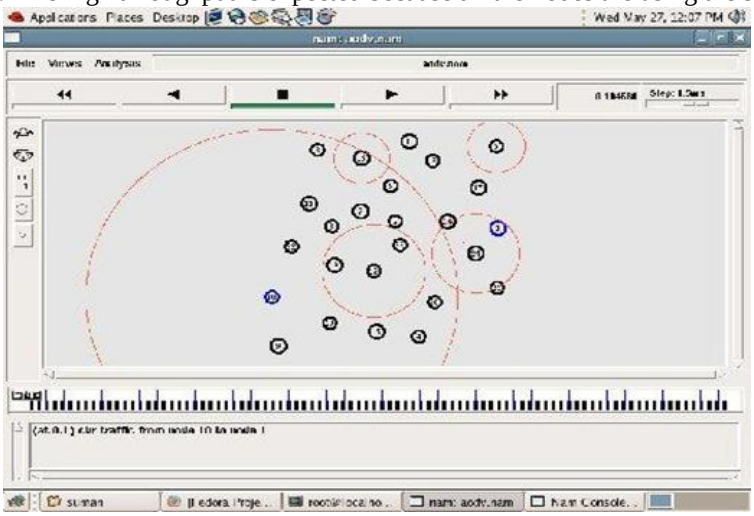


Fig. 6.1: Source node broadcasts RREQ

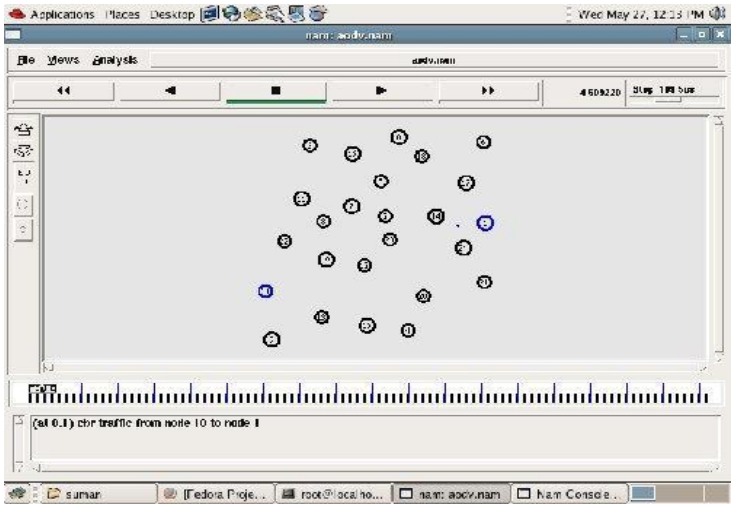
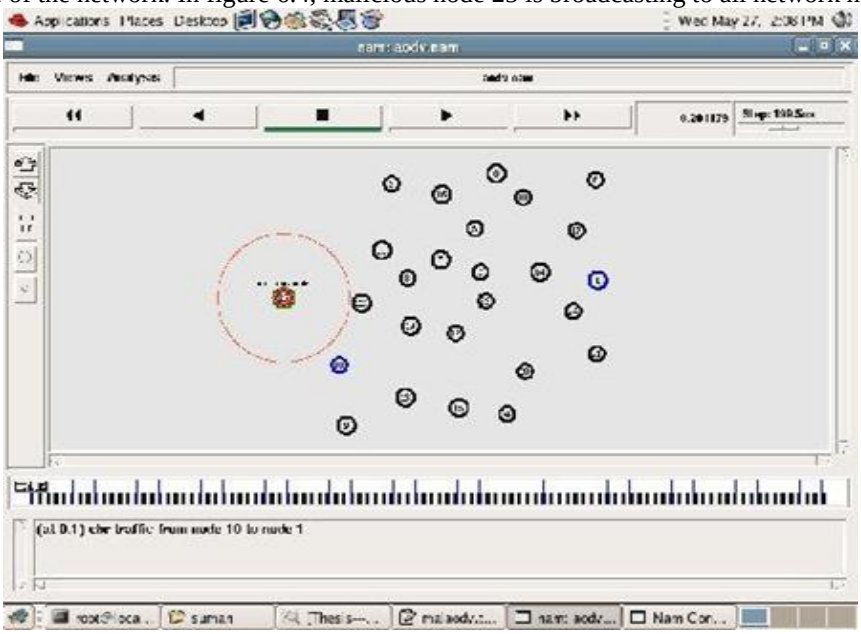


Fig. 6.2: Transmission of data packet

B. AODV with Malicious Node

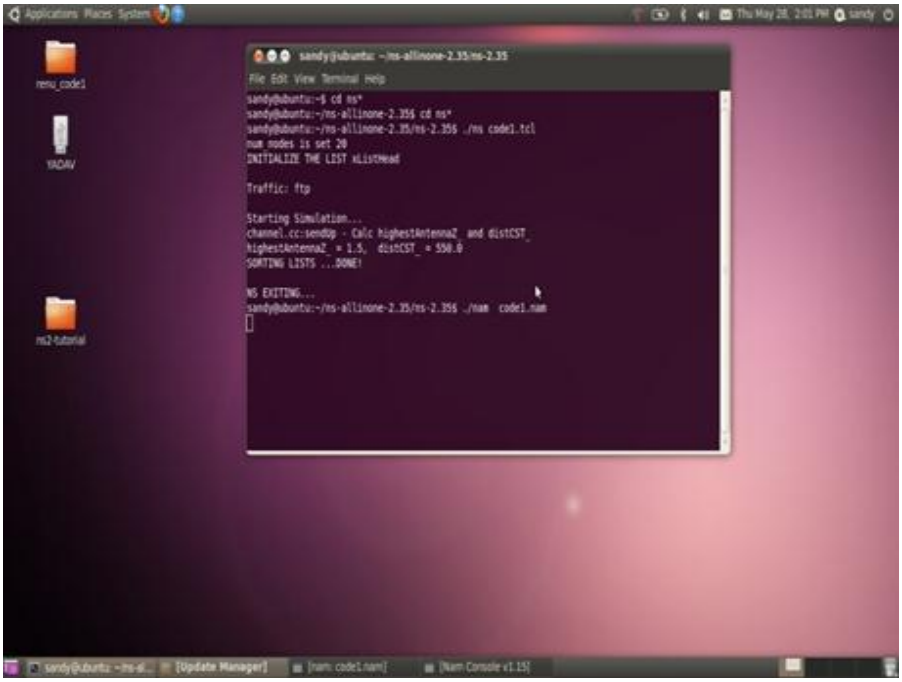
When malicious node (25) is inserted into the network as shown in the figure 6.4, it receives the broadcast packets and tries to behave like regular node of the network. In figure 6.4, malicious node 25 is broadcasting to all network nodes.



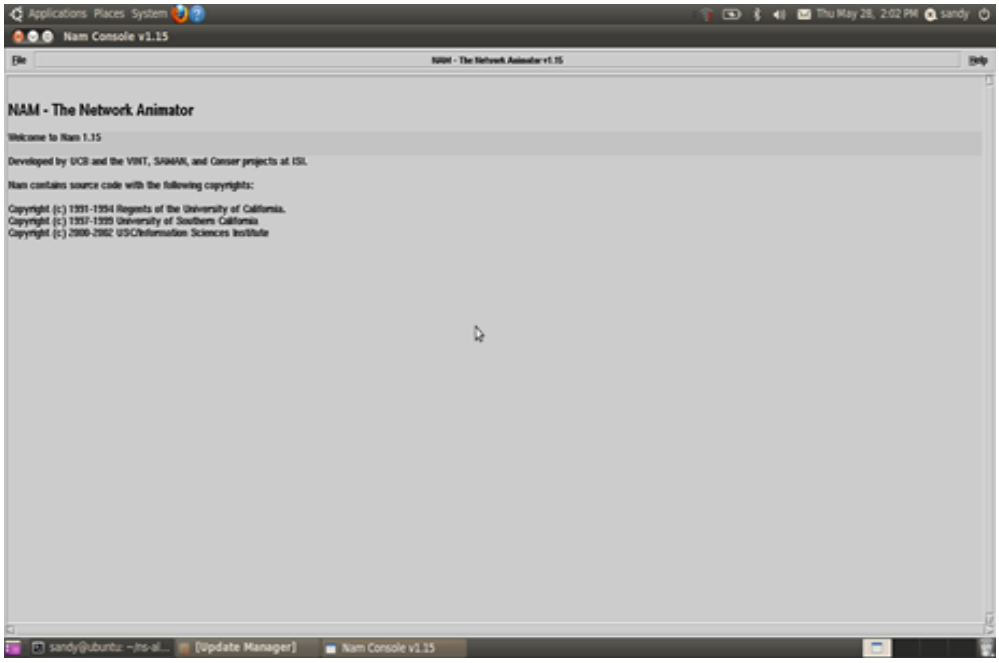
Now malicious node (25) receives RREP packet from the destination node and sends its own data to the destination node 1. In figure 6.5, malicious node and source node both are sending their own data to the destination node. The packet from malicious node is of black color and it sends more packets than source node. The malicious node tries to jam the channel by sending more and more packets so that the throughput decreases.

Here we use a new method for decreasing the packet loss rate and to increase the efficiency of the communication,by introducing a node which first examine its neighbor nodes for communication and then gets communicate with the nodes.
By applying this method the packet loss rate will decrease and the efficiency will increase.

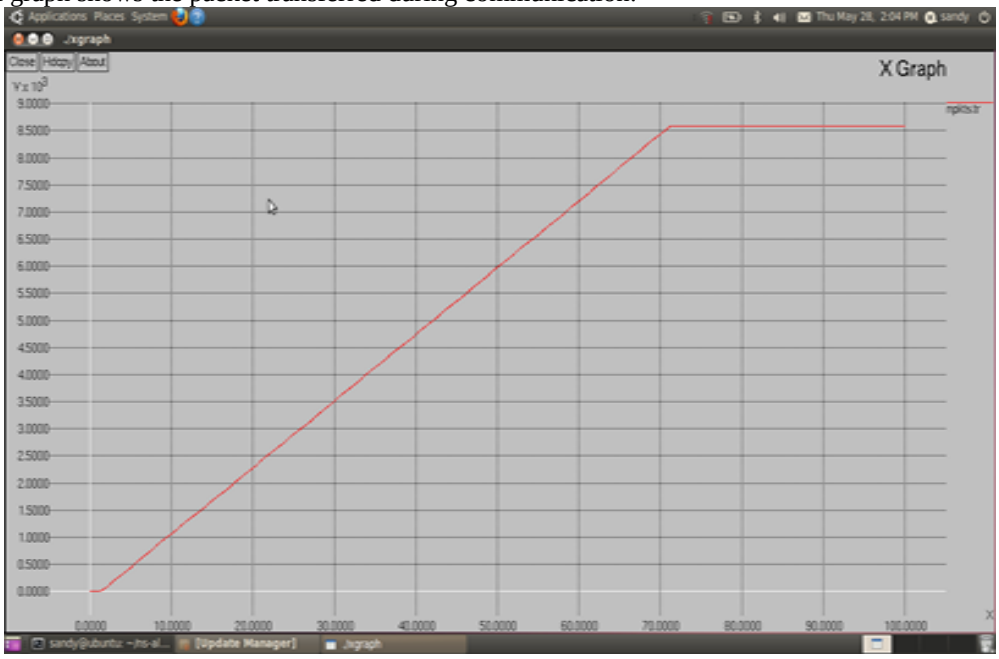
1) Firstly we generate the network animator in the terminal by running the code which is already in tool command language.



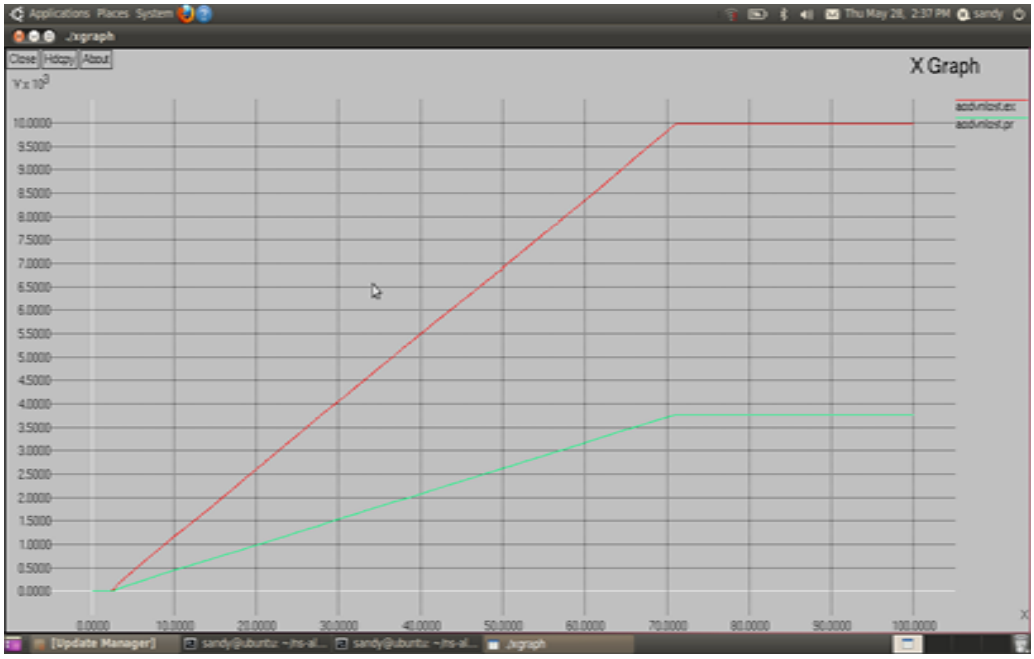
2) The second graph shows the generation of network animator:



3) The third graph shows the packet transferred during communication:



4) The fifth graph shows the difference of the packet loss rate between previous method and the new method.
5) The green line shows the packet loss during communication between nodes in the proposed method.
6) The red line shows the packet loss in previous method.



V. CONCLUSION

Security is a significant issue in Wireless Sensor Networks. Intrusion of malicious nodes may cause serious impairment to the security. The objectives listed have been carried out. In the presented work, we have discussed all the modes of AODV (simple mode, frequency hopping and malicious node) along with their working. We sincerely hope that our work will contribute in providing further research directions in the area of security based on frequency hopping.

In this thesis work, AODV over WSN is simulated with different operation modes. An important contribution of this thesis is the comparison of the WSN with and without malicious node using the frequency hopping technique.

With the results of AWK programming and tracegraph, we can conclude that in the case of simple AODV there is no packet drop and throughput is 100%. But when two frequencies are hopped in the network with different simulation times, throughput is less than 100% but increases continuously with respect to simulation time. After a simulation time of 2000 seconds (~33 minutes) almost 98 percent packets reach the destination safely.

As the malicious node enters into the network, it tries to capture the network. The performance of the network is affected badly. But, after applying frequency hopping, as the simulation time increases the throughput at the destination node also increases, which means that the network is secure enough to overpower the malicious node.

And In the new work it is said if we enter such a node that first identify all the neighbour nodes and then starts communication then it gives results as a less rate of packet loss during communication.

We can increase the efficiency of the previous work upto 40% and decrease the packet loss rate.

Practical WSN security is a balancing act that is constantly in search of the highest level of protection that can be squeezed out of the judicious use of limited resources. A large number of security problems are still open in WSN. One of the open problems is authentication of sensor nodes. To secure the sensor network when a new node enters into the network, it should be authenticated. Another, aspect of future research direction can be a non-beacon enabled WSN. Further, path hopping is another optional concept that can be used to secure the sensor network.

REFERENCES

[1] Chatschik Bisdikian, "An overview of the Bluetooth Wireless technology", IEEE Communication Magazine, vol. 39, Dec 2001.
[2] Brain P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks", IEEE Communication Magazine, Vol. 35, Sep 1997
[3] J. Macker and S. C. (chairmen). MANET (Mobile Ad Hoc Networking) working group of the IETF.
[4] K. Jones, A.Waada, S. Olaniu, L.Wison, M. Eltoweissy, "Towards a new paradigm for Securing Wireless Sensor Networks", New Security Paradigms workshop 2003, Ascona, Switzerland.
[5] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University.
[6] J. Zheng and Myung J. Lee (2006). A comprehensive performance study of IEEE 802.15.4 – Sensor Network Operations: Wiley Interscience. IEEE Press Chapter 4. 218-237.
[7] IEEE 802.15.4 WPAN-LR Task Group Website: http://www.ieee802.org/15/pub/
[8] 802.15.4: A Developing for Low Rate Wireless Personal Area Network".
[9] Anis Koubaa, Mario ALVES, Bilel NEFZI, Ye-Qiong SONG, "Improving the IEEE 802.15.4 Slotted CSMA-CA MAC for Time-Critical Events in Wireless Sensor Network".
[10] Anis Koubaa, Mario ALVES, Eduardo TOVAR, "A Comprehensive Simulation".
[11] Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks", in Mobile Computing and Networking, 2000, pp. 243–254.

[12] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communication Magazine, Aug. 2002.
[13] Dr. A.K. Verma, Mayank Dave, R C Joshi, "DNA-Cryptography a novel paradigm for securing MANETs", vol-11-2008, no-4PP-393-404" J. Discrete Mathematics Science & Cryptography.
[14] Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, "SPINS: security protocols for sensor networks", in: Proceedings of Mobile Networking and Computing 2001, 2001.
[15] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", University of California at Berkeley, Berkeley, CA 94720, USA, Ad Hoc Networks 1 (2003) 293–315.
[16] Intanagonwiwat, R. Govindan,
[17] and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00), August 2000.
[18] Elizabeth M. Royer, Charles E.Perkins, "An Implementation of the AODV Routing Protocols".
[19] Ad hoc on-demand distance vector (aodv) routing. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt.
[20] Teemu Vanninen, Hannu Tuomivaara, Juha Huovinen "A Demonstration of Frequency Hopping Ad Hoc and Sensor Network Synchronization Method on WARP Boards", WinTech'08, September 19, 2008, San Francisco, California, USA. ACM 978-1-60558-187-3/08/09.
[21] Ye, A. Chen, S. Liu, L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks", Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001.
[22] Ye, S. Lu, L. Zhang, "GRAdient broadcast: a robust, long-live large sensor network", Tech. Rep., Computer Science Department, University of California at Los Angeles, 2001.Braginsky, D. Estrin, "Rumour routing algorithm for sensor networks", in: First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
[23] Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks", Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.
[24] J. R. Douceur, "The Sybil Attack", in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.
[25] Roosta, T., Shieh, S. and Sastry, S. "Taxonomy of Security Attacks in Sensor Networks and Countermeasures". Berkeley, California, University Press, 2006.
[26] D. W. Carman, P. S. Krus, and B. J. Matt. "Constraints and approaches for distributed sensor network security". Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.