A SIMPLE AND EFFECTIVE SCHEME TO FIND MALICIOUS NODE IN WIRELESS SENSOR NETWORK

T.Sathyamoorthi[1], D.Vijayachakaravarthy[2], R.Divya[3], M.Nandhini[4]

[1,2,3] *Master of Engineering, Computer Science and Engineering, Parisutham Institute of Technology and Science, Tamilnadu, India*

Abstract

Wireless Sensor Network consists of hundreds or thousands of sensor nodes. Impractical to maintain topology and protect each sensor nodes from attack. Wireless Sensor Network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When sensor nodes are deployed in such an environment, sensor network lacks in physical protection and is subject to insertion of malicious node. After that an adversary may launch various attacks to disrupt the in-network communication through malicious node. In such attacks malicious node behave like normal nodes by selectively drop packets for make it harder to detect their malicious nature. Many schemes have been proposed to detect malicious nodes, but very few can identify attacks. But those proposals are send redundant packets, consume more energy and storage to identify malicious nodes. A simple and effective scheme proposed as Stop Transmit and Listen (STL) to find the malicious node. Each node is having the built-in time limit to stop their transmission. For every few seconds every node stops their transmission and listens for malicious behavior. Malicious nodes are not aware of non-transmitting time. If malicious node sends or forwards the data in non-transmitting time, malicious node is caught by their neighbor nodes in the network.

Key Words: *IDS, Secure Routing Protocol, Stop Transmit and Listen*

----------***----------

1. INTRODUCTION

A WSN consists of large number of autonomous sensor nodes, in which each and every sensor is connected with one or more sensor nodes without the use of any wires(i.e.) connected via wireless. The design of WSNs depends on required application. Environmental monitoring is an application where a region is sensed by numerous sensor nodes and the sensed data are gathered at the base station (a sink) where remaining process can be carried out. The sensor nodes for such applications are usually designed to work in conditions where it cannot be possible to recharge or refill the battery of those nodes. Hence energy is very precious resource for sensor nodes. This limitation makes the design of routing protocols a challenging task. The WSN is built of "sensor nodes" – from a few to some hundreds or thousands, where every node is connected to one or several sensors. Each sensor node have several parts such as a radio transceiver consisting internal antenna and an external antenna, an electronic circuit, a microcontroller and an energy source usually a battery.

Actually the nodes are referred as “Sensor” because these nodes are equipped with smart sensors. A sensor node is a device that converts a sensed characteristic like temperature, vibrations, pressure into a form recognize by the users. A wireless sensor networks node has less mobility compared to ad-hoc networks. So mobility in case of ad-hoc is more. In wireless sensor network data are requested depending upon certain physical quantity.

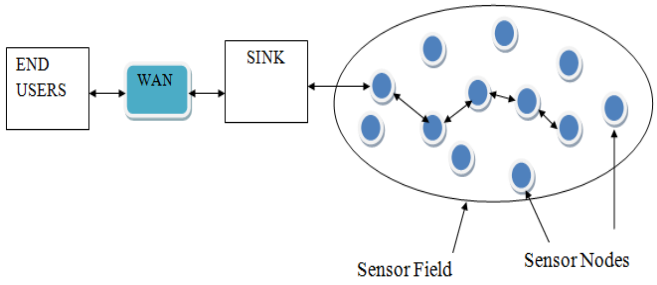

Fig -1: Wireless Sensor Network

Sensors are used to sense the data from the physical environment, memory is for storage, and a transceiver is used for data transmission. The main components of a sensor node as seen from the Fig.2 are power source, microcontroller, external memory, and transceiver one or more sensors. Microcontroller processes data and controls the functionality of other components in the sensor node.

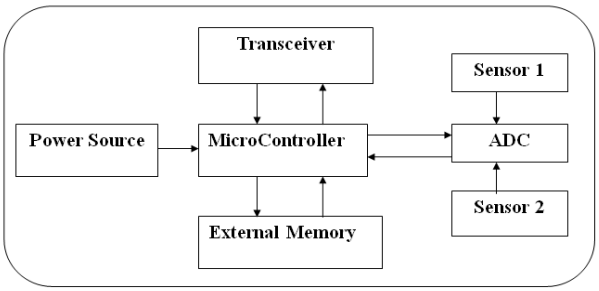

Fig -2: Architecture of Sensor Node

1.1 Security In Wireless Sensor Network

A wireless sensor network is a composed of large number of nodes that are densely deployed either inside the phenomenon or very close to it. It is spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions at different locations [8]. Wireless Sensor Network may operate in hostile environment, so security is needed to ensure the integrity and confidentiality of sensitive information. Security is important field in WSN and is quite different from traditional security mechanism. This is because of firstly, there are severe constraints on these devices namely their minimal energy, communicational and computational capabilities. Secondly, additional risk of physical attacks such as node capture and tampering.

1.2 Approaches To Detect malicious Node

Malicious nodes are act as legitimate node by selectively dropping the packets. More complex to find malicious nodes, if sensor nodes selectively dropping the packets. Various approaches are used to detect malicious nodes. The approaches are,

- Multipath forwarding
- Neighbor monitoring approach
- Acknowledgement based approach
- Node categorization and Ranking Algorithm

1.2.1 Multipath forwarding

In sensor network, sensed data forwarded through the multiple different paths. Even though malicious node is inside the network, by using the different paths the sensed data successfully forwarded towards the sink.

1.2.2 Neighbor monitoring approach

Nodes continuously monitor the forwarding behaviors of their neighbors to determine if their neighbors are misbehaving. In this method every nodes are having the capabilities of finding malicious node

1.2.3 Acknowledgement based approach

This method requires acknowledgement for every transmission to find malicious node. If acknowledgement not received for particular transmission then it confirms the malicious node intrusion. In this method source node finds the malicious node.

1.2.4 Node categorization and Ranking Algorithm

Each sender and forwarder adds a small number of bits called packet mark. Every node is categorized based on the packet marks. The sink periodically runs heuristic ranking algorithms to identify most likely bad nodes from categorization of nodes.

2. PROBLEM DEFINITION

Wireless Sensor Network consists of hundreds or thousands of sensor nodes. It is Impractical to maintain topology and protect each sensor nodes from attack. Wireless Sensor Network is often deployed in an unattended and hostile environment to perform the data collection and monitoring tasks. When wireless sensor network is deployed in such an environment, it has lacks of physical protection and is subject to insertion of malicious node. After that an adversary may launch various attacks to disrupt the in-network communication through malicious node. In such attacks malicious node behave like normal nodes by selectively drop packets for make it harder to detect their malicious nature.

Many schemes have been proposed to detect malicious nodes, but very few can identify attacks. But those proposals are send redundant packets, consume more energy and storage to identify malicious nodes. The existing approaches are delayed in finding the malicious node in sensor network. The storage overhead will affect the network due to unwanted transmission for finding malicious node. Large communication power is needed to detect the malicious node like acknowledgement and multipath forwarding.

3. PROPOSED SYSTEM

A simple and effective scheme proposed as Stop Transmit and Listen (STL) to find the malicious node. Initially, the sensor nodes are heavily deployed over the region. Each node is having the built-in time limit to stop their transmission. Each and every node is having the capability of finding malicious node. After the node deployment nodes are started their sensing process within their sensing region. The sensed data is forwarded towards the sink. For every few seconds every node stops their transmission and listens for malicious behavior. Malicious nodes are not aware of non-transmitting time.

If malicious node doesn't send or forwards the data in non-transmitting time, malicious node can be caught in other frequent non-transmitting times. If malicious node sends or forwards the data in non-transmitting time, it caught by their neighbor nodes in the network. Then malicious behavior of that node is broadcasted throughout the network. The malicious nodes are can be easily detected by neighbor nodes. So it is trusted method of malicious node detection.

3.1 Node deployment

Initially, the sensor nodes are heavily deployed over the region. Each node is having the built-in time limit to stop their transmission. Each and every node is having the capability of finding malicious node.

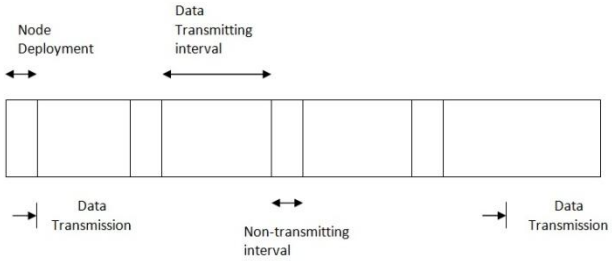

Fig -3: Operation time of STL

3.2 Data Transfer

After the node deployment nodes are started their sensing process within their sensing region. The sensed data is forwarded towards the sink. The proposed STL scheme doesn't need any type of network topology for data transmission.

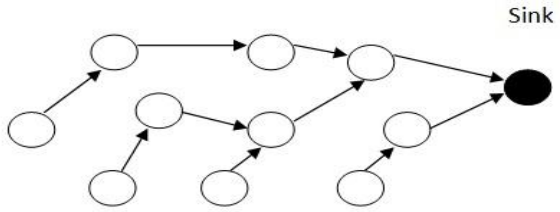

Fig -4: Data Transfer

3.3 Stop and Listen

For every few seconds every node stops their transmission. Malicious nodes doesn't aware of the non-transmission time allocation in the sensor nodes. So malicious may send or receive the data in non-transmitting time interval. Every node listens for malicious behavior in the non-transmitting time interval.

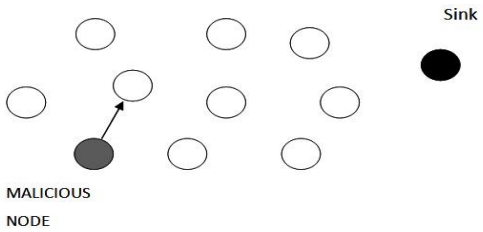

Fig -5: Non-transmitting intervals

3.4 Malicious node detection

Malicious node behaves like normal nodes by selectively nature. So malicious nodes send or forward the data in non-transmitting time interval. If malicious node doesn't send or forwards the data in non-transmitting time, malicious node can be caught in other frequent non-transmitting times. If malicious node sends or forwards the data in non-transmitting time, it caught by their neighbor nodes in the network.drop packets for make it harder to detect their malicious

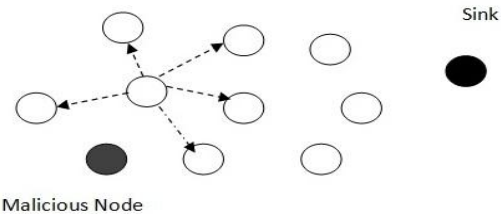

Fig -6: Broadcasting about malicious behavior

3.5 Malicious node Removal

Malicious behavior of the node is broadcasted throughout the network. Then every node in the network doesn't send data to the malicious node. A sensor node doesn't allow the data from malicious node. The malicious nodes are can be easily detected by neighbor nodes. So it is trusted method of malicious node detection.

4.CONCLUSIONS

Wireless Sensor Network is often deployed in an unattended and hostile environment to perform the data collection and monitoring tasks. When WSN is deployed in such an environment, it has lack physical protection and is subject to insertion of malicious node. Many schemes have been proposed to detect malicious nodes, but very few can identify attacks. But those proposals are send redundant packets, consume more energy and storage to identify malicious nodes. The proposed STL scheme is easily finds the malicious nodes in the network. It finds the malicious node in very short interval of time. It supports the malicious node detection in dynamic sensor network. Neighbor node detects the malicious node in the network. It doesn't any complex process to find. It is having the capability to find malicious nodes in sensor networks.

5.FUTURE ENHANCEMENTS

In the proposed STL scheme whole network data transmission is stopped for finding malicious behavior. In future, the whole sensor network will be separated into several groups. Each group is having the separate non-transmitting time. Each group stops their transmission in a non-overlapping time interval. The non-transmitting time is allocated hierarchically from the lower level nodes. If one group stops their transmission, other groups are sending and forward the data. The group separation overcomes the problem of congestion and delays in the sensor network.

REFERENCES

[1] Secure routing for mobile ad hoc networks, Proc. of the CNDS'02 (TX, San Antonio), January 2002.

[2] M. Burmester and T. van Le, Secure multipath communication in mobile ad hoc networks, Proc. of ITCC'04 (Las Vegas), IEEE, April 2004.

[3] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, Secmr- A Secure Multipath Routing Protocol for Ad Hoc Networks, Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

[4] R. Roman, J. Zhou, and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks," Proc.

IEEE Third Consumer Comm. Networking Conf. (CCNC), 2006.
[5] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," J. Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218-1230, 2007.
[6] X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Data Plane Security," Proc. ACM CONEXT Conf. (CoNEXT '08), 2008.
[7] "Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, Member, IEEE, and Wensheng Zhang, Member, IEEE Catching Packet Droppers and Modifiers in Wireless Sensor Networks may 2012.
[8] D. Djenouri, L. Khelladi, A.N. Badache, A survey of security issues in mobile ad hoc and sensor networks, Communications Surveys & Tutorials, Fourth Quarter 7 (4) (2005) 2–28.
[9] M.A.M. Vieira, D.C. da Silva Jr., C.N. Coelho Jr., and J.M. da Mata., "Survey on Wireless Sensor Network Devices," Emerging Technologies and Factory Automation (ETFA03), September 2003.
[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defense," International Symposium on Information Processing in Sensor Networks, Vol. 1(2004).
[11] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Journal of Ad Hoc Networks, Elsevier, 2003
[12] W. Du, L. Fang, and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," the 19th International Parallel and Distributed Priocessing Symposium (IPDPS'05), April 3 – 8, 2005, Denver, Colorado, USA.

BIOGRAPHIES

T.Sathyamoorthi is pursuing Masters Degree Program Department of Computer Science & Engineering, Parisutham Institute Of Technology and Science, affiliated to Anna University-Chennai, Tamilnadu, India. He received the BE degree from Kings College Of Engineering in 2012. His research interests include Mobile Ad-Hoc Network and wireless systems

R.Divya is pursuing Masters Degree Program Department of Computer Science & Engineering, Parisutham Institute Of Technology and Science, affiliated to Anna University-Chennai, Tamilnadu, India. She received the BE degree from Parisutham Institute Of Technology and Science in 2012. Her research interests include Cloud Computing.

Nandhini is pursuing Masters Degree Program Department of Computer Science & Engineering, Parisutham Institute Of Technology and Science, affiliated to Anna University-Chennai, Tamilnadu, India. She received the MCA degree from VLB Janakiammal College of Engineering and Technology in 2010.Her research interests include networks and cloud computing.

D.Vijayachakaravarthy is pursuing Masters Degree Program Department of Computer Science & Engineering, Parisutham Institute Of Technology and Science, affiliated to Anna University-Chennai, Tamilnadu, India. He received the BE degree from Kings College Of Engineering in 2012. His research interests include Mobile Computing.