IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Trustable and Secured Routing in Wireless Sensor Networks

[1] Muneebahmdhyiddeen; [2]Asha Paul; [3] Bastian Babu; [4] Dr. D. Loganathan

[1] Student, Final Year M.Tech - CSE, MET'S School of Engineering, Mala, Thrissur, Kerala, India

[2] Assistant Professor, Department of CSE, MET'S School of Engineering, Mala, Thrissur, Kerala, India

[3] Assistant Professor, Department of CSE, MET'S School of Engineering, Mala, Thrissur, Kerala, India

[4] Professor, Department of CSE, MET'S School of Engineering, Mala, Thrissur, Kerala, India

Abstract - Security is a serious issue in wireless sensor networks. Wireless sensor networks are widely used in variety of applications. In wireless sensor networks all the sensor nodes will works together with a goal to send the data to the destination without any fail. Because of their built in resource-constrained characteristics, they are vulnerable to various security attacks. A black hole attack is one of the serious insider attack in which the attacker compromises a node and drops all packets that are routed through this compromised node. It is a serious security attack which affects data collection. It may result in sensible data that will be eliminated or not able to be transmitted to the receiver node. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously it will make incorrect decisions. Therefore, how to detect and avoid black hole attack is of great significance for security in WSNs. This paper propose a secure and trustable routing of data using a mobile node. Thus ensures the enhancement of network lifetime and probability of successful routing.

Keywords - *Black hole attack, network lifetime, security, trust, wireless sensor networks*

1. Introduction

Wireless Sensor Networks are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. A wireless sensor network is a self-organizing network consisting of sensor nodes which can vary from hundreds to thousands in numbers. Each sensor node has restricted processing, storage capacity, computational power.

In wireless sensor networks, every sensor node communicates with other environment to know about its local environment and the data will send to any node if any requests are coming. In wireless sensor networks, it is not much secure when large area of network compared to small area of network [3]. Because of the inborn characteristics like memory limitations, open environment, power limitations and unattended nature, the security of a wireless sensor network is compromised [11]. These weak characteristics makes the network easily compromised by an adversary to make attacks resulting in disastrous consequences. Black Hole attack is one of the dangerous attack which exploits a trustworthiness of a network by promising routing of data packets to the destination knowing that it has a shortest path but in reality it drops all packets as well as selectively drops the packets, and consequently threatens reliability. As wireless sensor networks are causing many security threats, in this paper we are avoiding the black hole node by proposing a technique of data routing without any fail. The black hole attack gives the situation where an attacker trying to compromise some of nodes to track the information and interrupt with the normal working of the WSN by continuously changing, disturbing, or breaking the functionality of the nodes in the system. This attacks will results in generating the black holes: areas within which the adversary can either passively intercept or actively block information delivery. The attackers can provide many black holes due to the unattended nature of WSNs. By this attack adversary can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology.

To provide good solution to these problems, our cryptography-based security method is not enough. Because the attacker can take the encryption/decryption keys, once the particular node is compromised and can interrupt any information passed through the node. At the same time, an adversary can always perform certain form of black hole attack even if it does not have any knowledge of the crypto-system used in the WSN. The sensor nodes are randomly distributed in the area. The packet can sent to the destination node through the intermediate nodes, if the nodes are out of their sensing range. The term multi-hopping is used for the

packet transmission through intermediate nodes. As the wireless sensor networks are not the centralized system no need to set up an infrastructure. The wireless sensor networks have the end-to-end communication between the nodes. There is much research on black hole attacks [6]. Such studies mainly focus on the strategy of avoiding black Holes. In this paper we are dealing with a mobile node which helps a secure transmission of data.

2. Related Works

Anbuchelian. S et al proposed [1] an energy saving clustering algorithm for detecting the attacks on cluster heads and thus leads to the better energy consumption in the wireless sensor networks. Vipul Sharma et al [9] proposed a method for the detection and suppression of black hole attack in Leach based sensor networks. The aim for this research work is to advance a mechanism that can detect and overcome the effect of black hole attack in sensor network. The demerit in this paper was it will not detect the sensor nodes as a black hole node. Barleen Shinh proposed [2] a technique to detect and isolate the black hole attack. The proposed mechanism will detect the malicious node and freeze, it from the network. The methodology is based on the throughput of the network. When the throughput of the network, will decreases to certain threshold value, nodes in the network will go to head node and detect the malicious node. Single-path routing is an easy routing protocol but is quickly captured by the attacker.

Therefore, the best approach is via multi-path routing to the destination. Even if there is an attack in one route, the packet can securely reach the destination. Tao Shu propose [7] a randomized multi-path routing algorithm to detect black hole attack. Under the design, the routes taken by the "shares" of different packets change over time. So the attacker cannot track the routes gone by each packet if the routing algorithm becomes known to the attacker. Wenjing Lou propose and investigate a novel scheme, [4] Security Protocol for REliable dAta Delivery (SPREAD), to enhance the data confidentiality service in a network.

The proposed SPREAD scheme aims to provide further protection to secret messages from being compromised when they are delivered across the insecure network D Loganathan also propose [5] a hybrid multipath scheme (H-SPREAD) to improve both security and reliability of this task in a potentially hostile and unreliable wireless sensor network. The new scheme is based on a N-to-1 multipath protocol which helps to find multiple paths from every nodes to in one route discovery process. There are different multi-path route construction methods. H.-M. Sun [8] proposes a multi dataflow topologies (MDT) approach to resist the selective forwarding attack. In the MDT method, the network is divided into two topologies. If one topology failed to send the data, the destination will get the data through other topology. Yuxin Liu, [10] proposed an active trust scheme for secure and trustable routing in wireless sensor networks.

The paper proposes an active detection routing of data for better security and trust. The main goal of the scheme is to ensure that the nodal data safely reach the sink and are not blocked by the black hole. The detection route helps to find high trust node and in data routing, it will selects the route without black hole node and thus improve the success ratio of data reaching the sink. Even there is many research on black node attack and avoidance, there is still lots for further study.

3. Proposed System

In the proposed method we are introducing a mobile node to the network. In the above papers, they are discussed about different techniques of detecting black hole attack. As the black hole attack is a serious security attack which will totally destroy the operation of the network, we have to find an appropriate solution to the packet routing in the network.

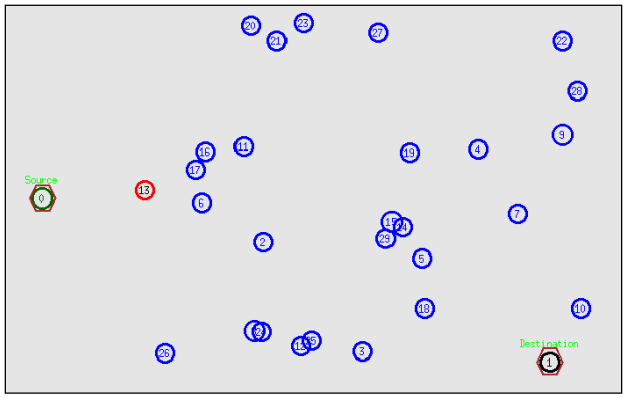

Fig.1: Drawback of existing System

Fig 1 shows the drawback of the existing system. In the existing system, the data will send through the trusted node in the network. For that they will first find the black hole attacked nodes for avoiding that nodes for the transmission of data. So there may be the situation that there will be not any good node between the sensing range of sender and destination. In such a situation the need for proposed system occurs. In our proposed method we are introducing a mobile relay node to the region where the data transferring is not occurring due to the black hole region. In all previous methods we are detecting the black hole nodes and freeze it from the networks. So the problem will occur when there no good nodes in the data route. When the black hole is

detected, nodes which are compromised will avoid from being data routing. As more and more black holes are detected, there may be the condition that destination node will not have any neighboring nodes in their range. Thus the data being sent to the destination will not reach there and network will die.

So our proposed method will help to avoid such situation. If any such situation occurs, the mobile node will occur in the network and move near to destination node for the smooth functionality of the network. The routing is done through AODV routing protocol for better performance.

Algorithm for Black hole detection

For each node in network
Check whether it is malicious or not
If node is malicious
Assign to M array
Else assign to T array

Data Routing

Check whether any trusted node is in between the sensing range of source and destination
If yes, send the data
Else
Select a trusted node
Make that node mobile
Move to an optimal position
Send the data.

Main aim of our proposed work is to make data route success probability high. That is safe landing of data to the destination without any hindrance in the route. The data may be corrupted or stolen by any compromised node in the network. So in our work, we are not sending the data through the black hole region. Also we are not sending the data through the uncompromised but untrusted node. There may be the case that there will be not any trusted node in the sensing range of sender and receiver. Fig 2 shows the secure data routing. The trusted powerful and energetic node in the network become a mobile node and move to an optimal position in the network. The four senders sending the data through different mobile nodes. So the Sender can send the network to the base station without any fail.

4. Implementation

Implementation is carried in NS2 platform. There are 50 number of nodes, which are deployed randomly and the destination is at the network's centre. In the existing method we can see that as more and more detection rounds are performed, the more black hole nodes are detected. And it may reduce the network life time and the probability of successful routing.

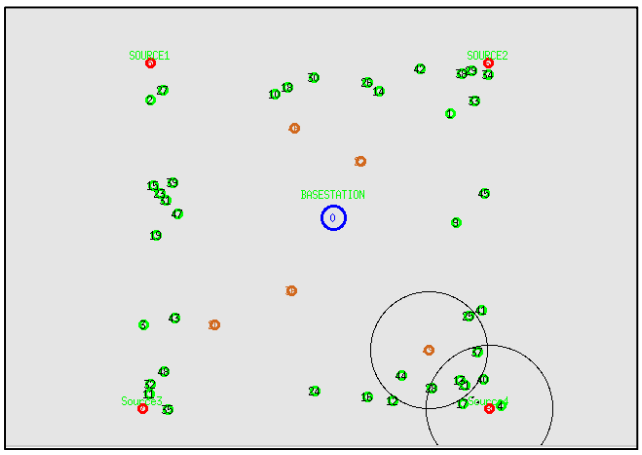

Fig 2: Secure Data Routing

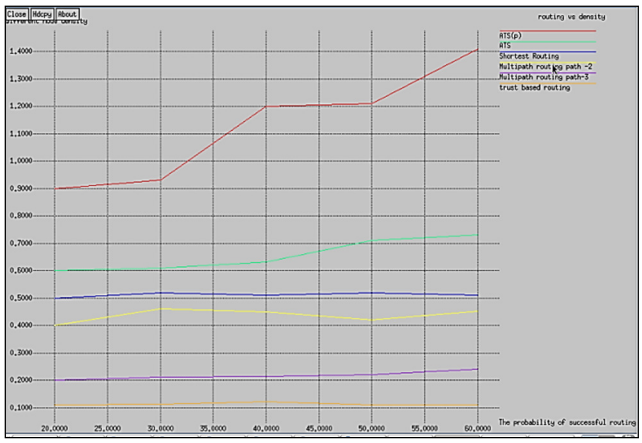

Fig 3: Probability of successful routing (different nodal densities)

As the main aim of our proposed method is secure routing of data, we have to ensure that the probability of successful routing should be high. In this method we are fixing four nodes as the senders to transmit the data.If any trusted nodes are not there in the sensing range of sender and the sink, the nodes in the network itself became mobile and move to an optimal position for the secure routing of the data to the destination Fig 3 shows the probability of successful routing under different nodal densities. As seen, when the nodal density grows, the nodal degree grows, and the probability of successful routing increases. The reason is that as the nodal density grows, the nodal degree grows, and then there are more detected trustable nodes after detection, that is, there are more nodes for the next hop, and the probability of successful routing thus increases.

Fig. 4 shows the probability of successful routing as the nodal transmission radius *r* grows as seen, the probability of successful routing is also increased. The reason is that, as *r* increases, the nodal density also increases, which is the same as found in the experiment of Fig 3.

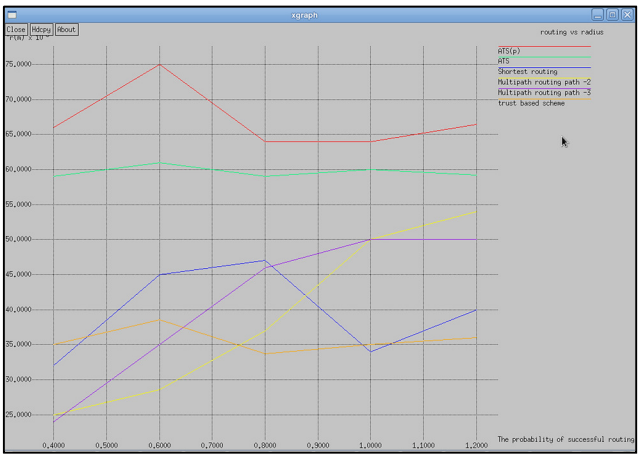

Fig 4: Probability of successful routing
(Different nodal transmission range)

5. Conclusion

In this paper, we have proposed a trustable and secure routing mechanism mainly aims at high successful routing probability, security and scalability. Our proposed scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. The proposed scheme also aims at high energy efficiency. It prevent the network being dead by providing a mobile node for the routing. Thus it will enhance the network lifetime. The analysis and result of our paper shows that our mechanism improves the successful routing probability. Further, it will also improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

References

[1] Anbuchelian, Selvamani. K, Chandarasekar. A "An Energy Efficient Multipath Routing Scheme by Preventing Threats in Wireless Sensor Networks", Electrical and Computer Engineering (CCECE), IEEE 27th Canadian Conference, 2014.

[2] Barleen Shinh "Novel Technique to Detect and Isolate Black hole Attack in MANET", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 6 June, 2014 Page No. 6513-6519.

[3] Liu A, M. Dong, K. Ota, and J. Long, "PHACK: An efficient scheme for selective forwarding attack detection in WSNs," *Sensors*, vol. 15, no. 12, pp. 30942–30963, 2015.

[4] Lou W, W. Liu, Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China,March 2004

[5] Loganathan, D, Ramamoorthy P,"Performance Enhanced in wireless Ad Hoc Networks Using Multicost Parameters Based Optimized Link State Routing Protocol", indianjournals.com , Vol. 6, No. 8, pp. 864-872. 2016

[6] Mitali Khandelwal, Sachin Upadhyay, "An Opinion Trust Based Detection and Prevention Method for Defending Black-hole and Gray-hole Attacks in Wireless Sensor Networks" , International Journal Of Scientific & Engineering Research, Volume 7, Issue 7, July-2016 .

[7] Shu.T, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010

[8] Sun H M, C.-M. Chen, and Y.-C. Hsiao, "An efficient countermeasureto the selective forwarding attack in wireless sensor networks," in *Proc.IEEE TENCON*, Oct./Nov. 2007, pp. 1–4.

[9] Vipul Sharma, KirtiPatil, Ashish Tiwari "Detection and Suppression of Blackhole Attack in Leach based Sensor Network", International Journal of Computer Technology and Applications, Vol 5 (6),1873-1877, 2014.

[10] Yuxin Liu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE, and Anfeng Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks" IEEE

[11] Zheng Z, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "Energy and memory efficient clone detection in wireless sensor networks," IEEE Trans. Mobile Comput, vol. 15, no. 5, pp. 1130–1143, May 2016.

Authors -

Muneebahmdhyiddeen received the B.Tech degree in Computer Science and Engineering from Calicut University, Kerala, India, in 2011, and currently doing M.Tech in Computer Science and Engineering in MET'S School of Engineering, Mala – Abdul Kalam Technological University, Kerala, India.

Asha Paul is an Assistant professor in MET'S School of Engineering Mala, Thrissur, Kerala. Received B.Tech degree in Information Technology from East Point College of Engineering, Bangalore and M.Tech from Karunya University, Coimbatore. She has more than 3 years of teaching experience. Subject of interest are Data Structures, Computer Organization and Design, Object Oriented Programming, C Programming and Digital Data Communication. She has presented paper on International Conferences.

Bastian Babu is an Assistant Professor in MET'S School of Engineering Mala, Thrissur, Kerala. Received B.Tech degree in Information Technology from Calicut University and M.Tech from Karunya University, Coimbatore. He has Published papers on International conferences.

Dr. D. Loganathan is a Professor and Head of Computer Science and Engineering department in MET'S School of Engineering, Mala, Trissur, Kerala. After his B.E., and M.E degree, he accomplished a doctoral degree from Anna University, Chennai, India. He has more than 20 years of teaching experience and having 8 years of research experience in engineering field. His research interest includes Wireless Communication, Wireless Ad hoc Networks and Image Processing. He has published several research papers in various international journals.