ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Secure and Reliable Black Hole Detection Attack and To Increase the Network LifeTime in Wireless Sensor Networks

K.Meena kumari[1], Dr.Shirina Samreen[2]

M.Tech Student, Department of CSE, Anurag Group of Institutions, Village Venkatapur, Mandal Ghakesar, Dist Medchal, Telangana, India[1]

Associate Professor, Department of CSE, Anurag Group of Institutions, Village Venkatapur, Mandal Ghakesar, Dist Medchal, Telangana, India[2]

ABSTRACT: Security is a serious issue in wireless sensor networks. Wireless sensor networks are widely utilized in form of applications. In wireless sensor networks all the sensor nodes will works along with a goal to send the information to the destination without any fail. Because of their in-built resource-constrained characteristics, they're vulnerable to varied security attacks. A black hole attack is one amongst the serious insider attack during which the attacker compromises a node and drops all packets that are routed through this compromised node. It's a significant security attack that affects information collection. It should result in sensible information that may be eliminated or unable to be transmitted to the receiver node. As a result of the network makes decisions depending on the nodes' sensed data, the consequence is that the network can fully fail and, additional seriously it'll build incorrect choices. Therefore, how to detect and avoid black hole attack is of great significance for security in WSNs. This paper proposes a secure and trustable routing of information using a mobile node. Therefore ensures the improvement of network lifetime and probability of successful routing.

I. INTRODUCTION

Wireless sensor networks (WSNs) have attracted a large range of disciplines sensor node interactions with the physical world are essential. Wireless network consisting of spatially distributed autonomous devices exploitation sensor to monitor the physical or environmental conditions. The sensor network consists sensor node, i.e. small, light-weight and portable. The most task of WSN is to sense and collect data, method and transmit in to the sink. WSN application and communication are in the main providing the high energy efficient. Wireless communication paradigm makes WSNs an important part of our daily lives. WSNs are composed of individual embedded system that's capable of interacting with their surroundings through varied sensors, processing data regionally and communication this with their neighbors. WSN application are space, health care and air pollution observation, environmental/earth sensing, forest fire detection, landslide detection, information work then on. Routing is that the method of choosing the most effective ways in a network. Router performs the traffic direction operate on the net. A router has 2 stage of operation they're control plane and forwarding plane. In control plane, a router maintain a routing table list a route should be wont to forward an information packet and thru physical interface connection. In forwarding plane, a route forward information packet between incoming and outgoing interface connection. The routing techniques are classified into 3 classes they are flat, hierarchical and placement primarily based routing. Router may offer property among and between enterprises and the net or between net service supplier's networks. The foremost powerful routers area unit typically found in ISPs; Routing is performed for several sorts of networks including the general public switched phone network (circuit switching), electronic information networks and transportation networks. Trust on the behavior of the component of the network is key side of WSN. Trust management system for WSN could be terribly helpful for detecting misbehaving nodes and for helping the choice creating method. Trust is an important issue of social and computing network

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

environment. The success of trust is looking on the adopting of the right approach for trust management system of WSN. Trust management system is often classified into 2 categories: credential-based trust management system and behavior-based trust management system. Trust management improves the protection of WSN.

II. RELATED WORK

Anbuchelian. S et al proposed an energy saving clustering algorithm for detecting the attacks on cluster heads and so results in the higher energy consumption within the wireless sensor networks. Vipul Sharma et al proposed a method for the detection and suppression of part attack in Leach primarily based sensor networks. The aim for this research work is to advance a mechanism that may detect and overcome the result of black hole attack in sensor network. The demerit during this paper was it'll not detect the sensor nodes as a black hole node. Barleen Shinh proposed a technique to notice and isolate the part attack. The proposed mechanism can notice the malicious node and freeze, it from the network. The methodology is predicated on the turnout of the network. Once the turnout of the network, can decreases to certain threshold price, nodes in the network can visit head node and notice the malicious node. Single-path routing is a simple routing protocol however is quickly captured by the attacker. Therefore, the simplest approach is via multi-path routing to the destination. Although there's an attack in one route, the packet can firmly reach the destination. Tao Shu proposes a randomized multi-path routing rule to notice black hole attack. Below the planning, the routes taken by the "shares" of various packets modification over time; so the attacker cannot track the routes gone every packet if the routing rule becomes better-known to the attacker; Wenjing Lou propose and investigate a completely unique scheme, Security Protocol for Reliable information Delivery (SPREAD), to enhance the data confidentiality service in an exceedingly network. The planned spread scheme aims to produce more protection to secret messages from being compromised when they are delivered across the insecure network D Loganathan additionally propose a hybrid multipath theme (H-SPREAD) to enhance each security and responsibility of this task in an exceedingly potentially hostile and unreliable wireless device network. The new scheme is predicated on an N-to-1 multipath protocol that helps to seek out multiple ways from each node to in one route discovery method. There are totally different multipath route construction ways. H.-M. Sun proposes a multi dataflow topologies (MDT) approach to resist the selective forwarding attack. Within the MDT technique, the network is split into 2 topologies. If one topology failed to send the information, the destination can get the information through different topology. Yuxin Liu, proposed an active trust scheme for secure and trustable routing in wireless sensor networks. The paper proposes an active detection routing of information for better security and trust. The most goal of the scheme is to ensure that the nodal information safely reach the sink and aren't blocked by the black hole. The detection route helps to find high trust node and in information routing, it'll selects the route without black hole node and so improve the success magnitude relation of data reaching the sink. Even there's several analysis on black node attack and avoidance, there's still lots for more study.

III. FRAME WORK

An overview of the active trust scheme that consists of an active detection routing protocol and information routing protocol is shown in Fig. 1

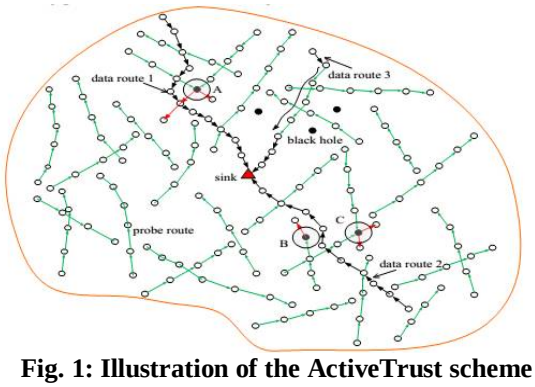


Fig. 1: Illustration of the ActiveTrust scheme

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

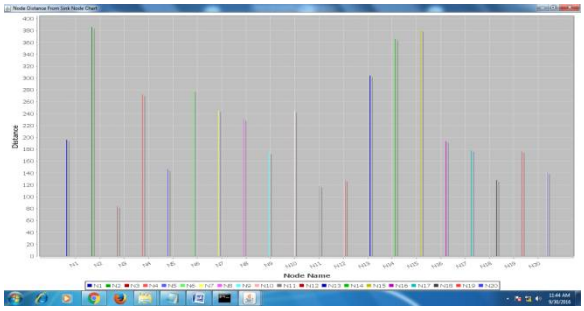
Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Active detection routing protocol is A detection route refers to a route while not information packets whose goal is to win over the adversary to launch an attack therefore the system will determine the attack behavior then mark the region location. Thus, the system will lower the trust of suspicious nodes and increment the trust of nodes in winning routing routes. Through active detection routing, nodal trust may be quickly obtained, and it can effectively guide the information route in selecting nodes with high trust to avoid black holes. The active detection routing protocol is shown via the green arrow in Fig. 1. During this scheme, the source node every which way selects an undetected neighbor node to create a lively detection route. Considering that the longest detection route length is, the detection route decreases its length by one for each hop till the length is shriveled to zero, and then the detection route ends. Information routing protocol is the information routing refers to the process of nodal information routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route can choose a node with high trust for the next hop to avoid black holes and therefore improve the success ratio of reaching the sink. The data routing is shown via the black arrow in Fig. 1. The routing protocol will adopt an existing routing protocol, and we take the shortest route protocol as an example. Node a in the route can opt for the neighbor that's nearer the sink and has high trust because the next hop. If there's not a node among all neighbors nearer the sink that has trust on top of the default threshold, it'll report to the higher node that there's no path from a to the sink. The higher node, operating within the same manner, can re-select a special node from among its neighbors nearer the sink till the information is routed to the sink or there's conclusively no path to the sink.

IV. EXPERIMENTAL RESULTS

The number of nodes to be created into the network and the energy assigned for each node initially. Route detection, each node in the network establishes a route to the sink node by using intermediate relay nodes. Initially the trust level and energy values for all the nodes is 10 and 100 respectively, if any nodes involves in route detection using intermediate nodes then its energy will be consumed in results. Select some sender node then send the data to the sink node from the selected sender. Here the data will send from N1 to N3 and then N3 to the sink node view trust to view the trust and energy values of all the nodes. Here both N1 and N3 are involved in transmission so their energy values are reduced Click on distance chart, here it will shows the distance between each node to the sink node



Generate blackhole to make a node as black hole in the network. In this, N1 has become as a black hole node and the route detection will happens for all the nodes. Select some sender node then send data. Here we are trying to send the data from N4, the path for this is N4, N1, N9, N18 and N3. The data transmission will fails as black hole attack existed in the path. Sending data from N5, N11, N20, and N3 to the sink node;

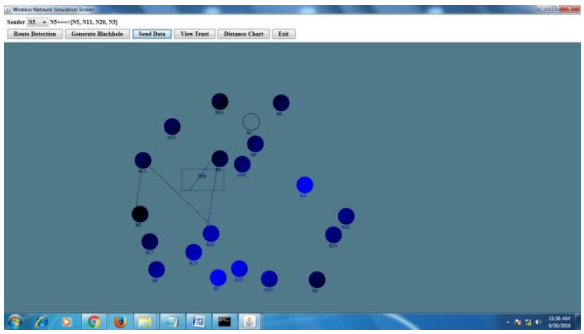
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017



V. CONCLUSION

In this paper, we have proposed a trustable and secure routing mechanism in the main aims at high successful routing probability, security and scalability. Our planned theme can quickly detect the nodal trust so avoid suspicious nodes to quickly achieve an almost 100% successful routing probability. The proposed scheme additionally aims at high energy efficiency. It prevents the network being dead by providing a mobile node for the routing. So it will enhance the network lifetime. The analysis and results of our paper shows that our mechanism improves the successful routing probability.

REFRENCES

1. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.
2. M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.
3. S. He, J. Chen, F. Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931 -1942, 2013.
4. X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016.
5. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.
6. A. Liu, M. Dong, K. Ota, et al. "PHACK : An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.
7. A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Information Sciences, vol. 230, pp.197-226, 2013.
8. Z. Zheng, A. Liu, L. Cai, et al. "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp. 1130-1143, 2016.
9. T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941 -954, 2010.
10. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.