International Journal of Research Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

An Recital Analysis Of Secure And Trustable Routing In Wireless Sensor Networks

A.Kalpana[1], G.Sushma [2]
[1]Assistant professor, Dept. of CSE, Ramanandha Tirtha Engineering college, India
[2] Assistant Professor, Dept. of CSE , Ramanandha Tirtha Engineering college, India

Abstract: A Wireless Sensor Network (WSN) has a wide range of application, gradually flattering an integral part of the living life. Wireless means the node can communicate without any physical media, i.e., the data is transmitted from one node to another in the form of packet. The topology of the WSNs can vary from a flat network to an advanced multi-hop wireless network. They are susceptible to to various security attack, a black hole attack is a type of attack that earnestly affect the data gathering. Find shortest path routing between source and designation is most challenging .To overcome that problem an active detection based security and trust routing scheme for proposed system to discovery out shortest path for secure communication.

Keywords- Black hole attack, Network lifetime, security, Trust, Wireless Sensor Network

I. INTRODUCTION

Wireless sensor networks (WSN) are distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to base station. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance[1]. Today wireless sensor networks are used in many applications, such as industrial process monitoring and control, machine health monitoring, and so on. In spite of all the advantages and applications of Wireless Sensor Networks, there are even some challenges and issues which have to be dealt with the WSN. The most key challenge is its security. There are various kinds of attacks in WSN like Grey hole attack, Wormhole attack, Sinkhole attack, Selective forwarding attack, Black hole attack, Denial of service attack etc. which will affect the data collection during routing process.

Routing Protocols [12] are generally classified into three types such as Proactive (Table Driven), Reactive (On Demand) and Hybrid based on route discovery process and their mechanism. The Proactive routing protocols select the routes to all destinations at beginning and maintain using periodic update process based on their mechanism. e.g. DSDV. The disadvantages of these algorithms are to update the routing tables often which take a large amount of memory, bandwidth and power. But, in the reactive routing protocol, there is no need to maintain the routing data in routing table by each node. The routes are selected and maintained only when they are required by the source for data transmission during route discovery process and the routing overhead has been reduced. e.g. Dynamic Source Routing (DSR) and Adhoc on Demand Distance Vector (AODV). The merits of both proactive and reactive protocols are combined and form a hybrid routing protocols e.g. ZRP, TORA.

Trust on the behavior of the element of the network is key aspect of WSN. Trust management system for WSN could be very useful for detecting misbehaving nodes and for assisting the decision making process. Trust is an important factor of social and computing network environment. The success of trust is depending on the adopting of the correct approach for trust management system of WSN [10]. Trust management system can be classified into two categories: credential-based trust management system and behavior-based trust management system. Trust management improves the security of WSN.

II. RELATED WORKS

Yuxin Liu et al. [1] have supplied the Active Trust approach for WSN. This method avoids black holes via retaining track in their quantity and obtains a trust version. Thus the approach improves the data direction security. ActiveTrust can extensively improve the statistics path success opportunity and potential against black hole attacks and can optimize network lifetime. The ActiveTrust scheme is the primary routing scheme that makes use of active detection routing to address Black hole Attack. The counseled routing protocol has higher power performance and protection overall performance. ActiveTrust scheme designs the Active detection routing protocol that can be to pick out the attack behavior and then mark the black hollow region and records routing protocol refers back to the system of nodal data routing to the sink. It selects a node with excessive consider for the subsequent hop to avoid black holes and enhance the success ratio of achieving the sink. ActiveTrust has the extreme a success routing probability, protection and scalability and high strength performance.

R. K. Bar et al. [2] have suggested the trust based AODV routing protocol by means of exclusion of Black Hole Attack. In the AODV routing protocol a course is selected in this type of manner that greater depended on nodes are involved. A Trust cost for each node is calculated relying upon the packet forwarding potential and weight factor of the node. A rank is generated based totally in this trust cost. Weight issue is described because the ratio of number of RREP set to the variety of RREQ obtained by using the node. Trust cost is inserted in the routing desk and the route discovery is executed according to this agree with cost by means of averting a less relied on node.

1) Calculate the Threshold Value W_1=N_o. of packet send/No. of packet received

2) Calculate the Weight Factor

W_2=N_o of RREP send/N_o. of RREQ received Increase the ptrust value while price is greater than the threshold price, in any other case decrease the ptrust price. Three) Calculate Trust Value= $W_1*W_2*p_{trust}$ Depending upon the accept as true with cost and the threshold value the black hole node is identified and it's far excluded from the direction established order manner. It keep away from the low relied on nodes, the average packet lack of the network is also decreased significantly. Thus the best of provider of the network is better in case of packet loss.

Satyajayant Misra et al. [3] have provided BAMBi technique to successfully mitigate the unfavourable results of black hole attacks on WSNs. Black hole attacks occur whilst an adversary captures and re-applications a set of nodes in the community to drop the packets. BAMBi is based totally on the deployment of a couple of base stations within the network and routing of copies of data packets to these base stations and the solution is rather powerful and requires very little computation and message exchanges inside the network, therefore saving the energy of the SNs. This approach can obtain greater than 99% packet delivery achievement and prove that the scheme can pick out a 100% of the black hollow nodes.

Praveen K S et al. [4] have as compared AODV and OLSR routing protocols for studying the Black Hole Attack in Ad Hoc network. Here, the authors have proven that the attacker node waits for the neighboring node to initiate the RREQ (path request) packet. The attacker gets the request, and sends the fake respond packet RREP (route reply) with a brand new sequences variety. Thus the attacker takes control of the routing path and thereby reduces the throughput. Throughput is the total number of packets despatched effectively from sender to receiver in a particular time. Throughput consequently computed is used because the metrics to locate presence of attacks.

R. Kompella et al. [5], gift a easy and effective approach to detect and diagnose the silent screw ups, i.e. data packets are silently dropped within the network with out giving any responses. This technique makes use of lively dimension between area routers to raise alarms each time end to stop connectivity is disrupted. In this the tier-I ISP community successfully stumble on and localize the black holes. The authors consciousness on detection and localization of silent faults bobbing up from the interplay between MPLS and IP layers of backbone networks. Using real failure data obtained from the tier-1 network's IPFM and MPFM systems, tested that each systems can correctly aid network operators in troubleshooting failures.

D. He et al. [6], have proposed the ReTrust (Attack-Resistant and Lightweight Trust) for wireless MSD (Medical sensor Networks). The authors have identified the security and overall performance challenges dealing with a sensor network for wireless scientific tracking and suggest the two-tier structure, based at the architecture develop the ReTrust. ReTrust no longer handiest can effectively discover malicious behaviors, but can also considerably enhance the network performance. ReTrust work with topologies intracell and intercell topology. ReTrust is viable for reinforcing the security and network performance of real MSN applicarions.

III. PROPOSED SYSTEM MODEL

An overview of the Active Trust scheme, which is composed of an active detection routing protocol and data routing protocol, is shown in Fig. 1. Active detection routing protocol: A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behavior and then mark the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active detection routing, nodal trust can be quickly obtained, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes.

The active detection routing protocol is shown via the green arrow in Fig. 1. In this scheme, the source node randomly selects an undetected neighbor node to create an active detection route. Considering that the longest detection route length is , the detection route decreases its length by 1 for every hop until the length is decreased to 0, and then the detection route ends. (2) Data routing protocol. The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs [3, 7, 8]; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink. The data routing is shown via the black arrow in the Fig.1. The routing protocol can adopt an existing routing protocol [7, 8], and we take the shortest route protocol as an example. Node a in the route will choose the neighbor that is nearer the sink and has high trust as the next hop. If there is not a node among all neighbors nearer the sink that has trust above the default threshold, it will report to the upper node that there is no path from a to the sink.

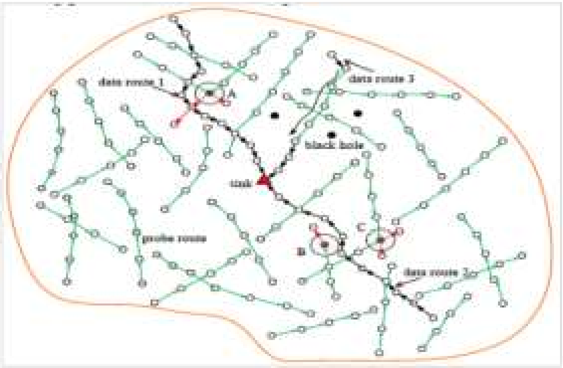

Fig.1: Illustration of the Active Trust scheme

The upper node, working in the same manner, will re-select a different node from among its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink. The network radius R=500 m, there are a total of 1000 nodes in the etwork, among which there are 300 black nodes, nodes are randomly and uniformly deployed, and the sink is at the network's center.

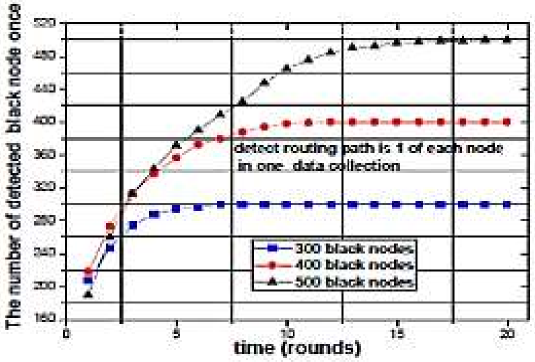

Fig. 2 : The number of detected black nodes as the network operates

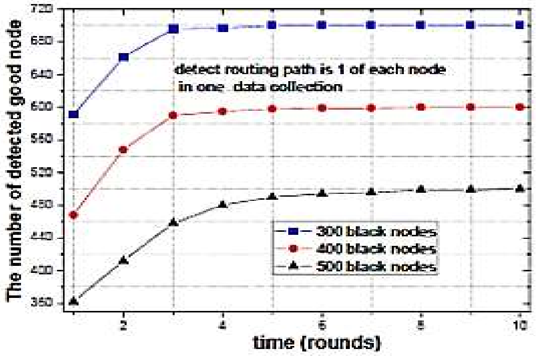

Fig. 3 : The number of detected good nodes as the network operates.

The investigational scene in Fig. 2 is such that in each data collection round, each node initiates one detection route with a length of 5. As seen, as the network runs, i.e., as more detection routes are performed, the number of black nodes detected grows quickly; when Fig. 3 shows the number of detected good nodes as the network runs in the same experimental scene as in Fig. 2 as seen, after only 4 rounds, our Active Trust scheme has detected all of the good nodes because in the data routing, it needs only one good downstream node to route the next hop; this indicates that, according to our scheme, the route can be reliable and have a high success probability.

IV. CONCLUSION

In this paper, we have proposed a novel security and trust routing scheme based on active detection, and it has the following excellent properties: (1) High successful routing probability, security and scalability. The Active Trust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. (2) High energy efficiency. The Active Trust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that our scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases.

REFERENCES

[1] Yuxin Liu, Mianxiong Dong Ota, Kaoru and Anfeng Liu," ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transaction on information forensics and security, sep 2016, Vol.11, No.9.

[2] R. K. Bar, J. K. Mandal, and M. Singh," QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", International Conference on Computational Intelligence: Modeling Techniques and Applications, India (CIMTA), Elsevier Procedia Technology 2013,vol. 10, pp. 530-537.

[3] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue," BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", Publication in the IEEE International Conference on Communications (ICC), 2011, pp 1-5.

[4] Praveen K S, Gururaj H L,Ramesh B," Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols", International Conference on Computational Modeling and Security (CMS 2016), Elsevier Procedia Computer Science, vol. 85, pp. 325–330.

[5] R. Kompella, J. Yates, A. Greenberg, and A. Snoeren. "Detection and localization of network black holes". In Proceedings of IEEE INFOCOM, 2007, pages 2180– 2188.

[6] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust:Attack-resistant and lightweight trust management for medical sensor networks," IEEE Trans. Inf. Technol. Biomed, Jul. 2012, vol. 16, no. 4,pp. 623–632.

[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.

[11]. S. Shen, H. Li, R. Han, et al. "Differential game-based strategies for preventing malware propagation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol.9, no. 11, pp. 1962-1973, 2014.

[12]. O. Souihli, M. Frikha, B. H. Mahmoud, "Load-balancing in MANET shortest-path routing protocols," Ad Hoc Networks, vol. 7, no. 2, pp. 431-442, 2009.

[13]. J. Long, A. Liu, M. Dong, et al. "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," Journal of Parallel and Distributed Computing, vol. 81, pp. 47-65, 2015.

[14]. S. He, J. Chen, X. Li, et al. "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE transactions on mobile computing, vol. 13, no. 6, pp.1268-1282, 2015.

[15]. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2014.