Trust based Routing to Detect Black Hole Attacks in Wireless Sensor Networks – A Survey

Vinitha M[1] Dr. Anitha Julian[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Velammal Engineering College, Chennai India

Abstract— A Wireless Sensor Network (WSN) has a wide range of application, slowly becoming 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. WSN is being deployed for many real time applications where the dynamical monitoring of sensed data is required. Sensor networks are application-specific and the routing of data between the sensor nodes has to be without interruption and errorless. Routing protocols try to incorporate methods to ensure avoidance of misbehavior of intermediate nodes. The trust among the distributed network is generally used as a powerful tool to improve the performance of sensor networks. This paper presents a detailed survey on the security and trust communication between the sensor nodes with routing techniques to detect and prevent data packet from the being exposed to Black hole attack. The paper also concludes with a comparison among the existing works.

Key words: Wireless Sensor Network, Routing, Trust, Black Hole Attack

I. Introduction

Wireless sensor networks (WSNs) have attracted a wide range of disciplines sensor node interactions with the physical world are essential. Wireless network consisting of spatially distributed autonomous devices using sensor to monitor the physical or environmental conditions. The sensor network consists sensor node, i.e. small, lightweight and portable. The main task of WSN is to sense and collect data, process and transmit in to the sink. WSN application and communication are mainly providing the high energy efficient. Wireless communication paradigm makes WSNs an important component of our daily lives. WSNs are composed of individual embedded system that is capable of interacting with their environment through various sensors, processing information locally and communicating this with their neighbors [8]. WSN application are area, health care and air pollution monitoring, environmental/earth sensing, forest fire detection, landslide detection, data logging and so on.

Routing is the process of selecting the best paths in a network. Router performs the traffic direction function on the internet. A router has two stage of operation they are control plane and forwarding plane. In control plane, a router maintain a routing table list a route should be used to forward a data packet and through physical interface connection. In forwarding plane, a route forward data packet between incoming and outgoing interface connection. The routing techniques are classified into three categories they are flat, hierarchical and location based routing [9]. Router may provide connectivity within and between enterprises and the internet or between internet service providers (ISP) networks. The most powerful routers are usually found in ISPs. Routing is performed for many kinds of networks including the public switched telephone network (circuit switching), electronic data networks and transportation networks.

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. Literary Survey

Yuxin Liu et al. [1] have presented the Active Trust method for WSN. This method avoids black holes by keeping track of their number and obtains a trust model. Thus the method improves the data route security. ActiveTrust can significantly improve the data route success probability and ability against black hole attacks and can optimize network lifetime. The ActiveTrust scheme is the first routing scheme that uses active detection routing to address Black hole Attack. The suggested routing protocol has better energy efficiency and security performance. ActiveTrust scheme designs the Active detection routing protocol that can be to identify the attack behavior and then mark the black hole location and data routing protocol refers to the process of nodal data routing to the sink. It selects a node with high trust for the next hop to avoid black holes and improve the success ratio of reaching the sink. ActiveTrust has the high successful routing probability, security and scalability and high energy efficiency.

R. K. Bar et al. [2] have suggested the trust based AODV routing protocol by exclusion of Black Hole Attack. In the AODV routing protocol a path is chosen in such a way that more trusted nodes are involved. A Trust value for each node is calculated depending upon the packet forwarding ability and weight factor of the node. A rank is generated based on this trust value. Weight factor is defined as the ratio of number of RREP set to the number of RREQ received by the node. Trust value is inserted in the routing table and the route discovery is done according to this trust value by avoiding a less trusted node.

1) Calculate the Threshold Value

W1=No. of packet send/No. of packet received

2) Calculate the Weight Factor

W2=No of RREP send/No. of RREQ received

Increase the ptrust value when value is greater than the threshold value, otherwise decrease the ptrust value.

3) Calculate Trust Value= W1*W2*ptrust

Depending upon the trust value and the threshold value the black hole node is identified and it is excluded from the route establishment process. It avoid the low trusted nodes, the average packet loss of the network is also decreased significantly. Thus the quality of service of the network is enhanced in terms of packet loss.

Satyajayant Misra et al. [3] have presented BAMBi technique to effectively mitigate the adverse effects of black hole attacks on WSNs. Black hole attacks occur when an adversary captures and re-programs a set of nodes in the network to drop the packets. BAMBi is based on the deployment of multiple base stations in the network and routing of copies of data packets to these base stations and the solution is highly effective and requires very little computation and message exchanges in the network, thus saving the energy of the SNs. This technique can achieve more than 99% packet delivery success and prove that the scheme can identify 100% of the black hole nodes.

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

Throughput= Packet Size*Received packets*8/100

OLSR is an optimized routing protocol for Mobile Ad hoc Network because messages are compacted and reduces the number of retransmission to flood these messages. OLSR is a table driven, proactive link state protocol. Each node calculates the best next hop for other nodes and MPR (Multi Point Relays) which are subsets of neighboring nodes. The main idea of MPR is reduce the flooding of broadcast messages in the network by minimizing duplicate retransmission messages. OLSR without black hole attack has maximum throughput. AODV uses Client-server method that is Request-reply method for finding a valid path between sources to destination. AODV is one of the on demand and typical routing protocol, higher the throughput higher the performance by using AODV protocol has better throughput as the packets are sent fast and overhead will is avoided due to the avoidance of black hole attack. The comparison shows that AODV throughput is better than OLSR protocol because all the nodes have to update the destination in the table whenever the path is made.

R. Kompella et al. [5], present a simple and effective method to detect and diagnose the silent failures, i.e. data packets are silently dropped inside the network without giving any responses. This method uses active measurement between edge routers to raise alarms whenever end to end connectivity is disrupted. In this tier-I ISP network successfully detect and localize the black holes. The authors focus on detection and localization of silent faults arising from the interaction between MPLS and IP layers of backbone networks. Using real failure data obtained from a tier-1 network's IPFM and MPFM systems, demonstrated that both systems can effectively 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 performance challenges facing a sensor network for wireless medical monitoring and suggest the two-tier architecture, based on the architecture develop the ReTrust. ReTrust not only can efficiently detect malicious behaviors, but can also significantly improve the network performance. ReTrust work with two topologies intracell and intercell topology. ReTrust is feasible for enhancing the security and network performance of real MSN applications.

T. Shu et al. [7], have developed the mechanisms that generate randomized multipath routes to minimize the end-to-end energy consumption under given security constraints. Multiple paths are computed in a randomized way to sent information packet, routes taken by various shares of different packets keep changing over time. The authors are specifically interested in combating two types of attacks: compromised node (CN) and denial of service (DOS) .In the CN attack, a subset of nodes to eavesdrop information. In the DoS attack, the normal operation of the network is ensured by actively disrupting, changing, or even paralyzing the functionality of a subset of nodes. The algorithms can be applied to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets.

III. CONCLUSION

The wireless sensor network have emerged as a promising technology due to their wide range of applications in industrial, environment monitoring, military and civilian domain. The main task of WSN is to sense and collect data, process and transmit their to the sink. This paper presents a detailed survey on the trust based routing techniques used for communication between the sensor nodes. One of the major security threats namely black hole attack has been taken for study and the techniques incorporated within the trust based routing to overcome such attacks have also been surveyed. The detection of these attacks has shown to improve the secure transmission of packets between the sensor nodes. Further scope based on this survey is to implement techniques to detect and prevent the other attack like selective forwarding attack, Sybil attack, and redirect attack and so on.

S. No	Methology	Attack Addressed	Metrics	Observations
1	ActiveTrust [1]	Black hole attack	Packet of detection route, feedback packet, maximum route length	100% successful routing probability.
2	BAMBi [3]	Black hole	False positive value, black hole	99% successful packet delivery and 100%

		attack	radius, packet deliver	detection of black hole nodes.
3	Trust based AODV [2]	Black hole attack	Trust value, threshold value and weight factor	Node is termed if it forwards at least 80% of the received packet
4	ReTrust [6]	Malicious nodes	Packet delivery radio(PDR)	PDR is at 89%
5	Tier I-ISP network [5]	Black hole attack	False positive value	Detection of black hole attack is 80% in tier I network and 100% in hypothesis algorithm

Table 1: gives an illustrative an overview on the trust based mythologies to detect black hole attack and also gives the detailed information on the attack addressed, metrics used and the result observed.

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] H.-M. Sun, C.-M. Chen and Y.-C. Hsiao, “An efficient countermeasure to the selective forwarding attack in wireless sensor networks,” in Proc.IEEE TENCON, Oct. /Nov. 2007, pp. 1–4.

[8] Ian F.Akyildiz, Mehmet Can Vuran,”Wireless Sensor Network Book”, A John Wiley and Sons Ltd Published 2010.

[9] Jamal N. AI-Karaki,Ahmed E.Kamal,”Routing techniques in wireless sensor networking: A Survey”, proceedings by the ICUBE initiative of lowa state university, IA 50011,2004.

[10] Sakshi srivastava, kushal johari,”A Survey on Reputation and Trust management in wireless sensor network”, proceeding in the IJSRET, Aug 2012, Vol 1, Issue 3pp 139-149.