International Journal of Trend in Research and Development, Volume 4(3), ISSN: 2394-9333
www.ijtrd.com

Black Hole Attack in Wireless Sensor Networks

[1]Ms. Pooja G M and [2]Mrs. Jebah Jaykumar,
[1]MTech Student, [2]Assistant Professor,
[1, 2]Department of CSE, B.N.M. Institute of Technology, Bangalore, India

Abstract- Wireless Sensor Network consists of spatially distributed autonomous sensors to monitor environmental or physical conditions and has many practical applications. WSNs are of interest to adversaries and they become susceptible to some types of attacks since they are deployed in open and unprotected environments. Due to the limited resources of WSNs, it is challenging to incorporate basic security features such as authentication, key distribution and privacy in WSNs. But, trust management that models the trust on the behavior of elements of the network, can be especially useful for a sensor network environment to enhance security. Trust management schemes that are targeted at sensor networks need to be lightweight in terms of computational and communication requirements, yet powerful in terms of flexibility in managing trust between nodes of heterogeneous deployment.

Key Words: *Black hole node, Active trust scheme, Trust, Data Routing.*

I. INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to monitor and react to environmental conditions and send the collected data to a command center using wireless channels. The hardware components of a sensor node include a radio transceiver, an embedded processor, internal and external memories, a power source and one or more sensors [1]. The primary security goals for sensor networks are confidentiality, integrity, availability and authentication of data [2]. It is possible that the emerging importance of sensor networks could be hindered by their inherent security problems. It is then imperative to provide a set of security primitives and services that can protect those networks and improve their robustness and reliability. Due to limited resources of WSNs, it is challenging to incorporate basic security functions such as authentication and privacy. As a result, wireless sensor networks are prone to different types of malicious attacks, such as denial of service, routing protocol attacks etc. Traditional crypto schemes are incapable of preventing such types of malicious attacks. Trust management, which models the trust on the behavior of the elements of the network, can be especially useful for a sensor network environment. However traditional trust management schemes developed for wired and wireless networks may not be suitable for networks with small sensor nodes due to limited bandwidth and memory constraints. Trust management can help improving the security of WSN. For example, for the routing process, sensor nodes might need to know which other nodes to trust for forwarding a packet. For sensing purposes a node might need to trust other neighboring nodes for checking anomalous measurements [3]. However, as sensor nodes are usually constrained devices, the trust management systems must be lightweight enough to provide a good performance without hindering the functionality of the system. This survey deals with various trust management schemes proposed for WSNs. Black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them.

This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

II. LITERATURE SURVEY

Researchers are developed various trust management schemes for WSNs. Some of the innovative approaches are described here.

A. Trust Management for Resilient Geographic Routing (TM-RGR) [4].

The authors propose an algorithm for location verification and trust model for avoiding attacks on geographic routing. The basic idea here is to favor well behaving honest nodes by giving them the credit for each successful packet forwarding while penalizing suspicious nodes that supposedly lie about or exaggerate their contribution to routing. If a node lies about its location, it is immediately excluded from the forwarding set. Honest node with good communication link to the destination will remain longer time in the forwarding set. After a node constructs a routing table, it monitors the behavior of its one hop neighbors to which it forwards the packets by using snooping or overhearing techniques. It is a very simple trust model. The calculation of trust update value takes less time. But the accuracy is less and the chance of false positives and false negatives are high.

B. Hybrid Trust and Reputation Management (HTRM) [5].

This paper proposes a hybrid trust management model that combines aspects from behavior based and certificate based approaches. Certificates signed by the online trust management authorities and behavior based trust are used for trust calculation. Trust of a node is evaluated after accumulating enough number of evidences from certificate authority or highly trusted nodes or from neighbors. Recommendations from highest referral nodes are collected if certificate authority's certificate is not suffice. When negative evidences are collected, a certificate or trust can be revoked. Trust association between trust issuer i and trust target j are based on the following combinations: (a) locally stored information of i on the role based trust associations that were established prior to deployment, (b) valid certificates that j can provide to i, (c) recommendations received for j upon request by third parties that i has a trust association with, and (d) behavior based trust evaluation by supervision nodes that i has a trust association with. The first two are the implicit recommendations from the network owner and trust managing authorities and the latter two are explicit ones.

The paper considers both direct and indirect observations to calculate the trust. But high computational power is needed for evaluating both behavioral and certificate validation.

C. Group Based Trust Management Scheme (GBTMS) [6].

In this paper, trust is evaluated for a group of sensor nodes instead of single sensor node. The authors propose a light weight algorithm which employs clustering. GBTMS works on two topologies:

1. Intra group topology where distributed trust management approach is used
2. Inter group topology where centralized trust management approach is used.

GBTMS calculates the trust values based on direct and indirect observations. Direct observations represent the number of successful and unsuccessful interactions between nodes and indirect observations represent the recommendations of trusted peers about a specific node. Each cluster head evaluates other cluster heads and sensor nodes under its cluster. The main advantage of this method is that memory consumption is less since it uses unsigned integer trust value and trust of a group of nodes are evaluated. But the amount of resources and power needed are more since it relies on broadcast based strategy and also the trust is calculated based on the past interaction experiences in message delivery. A node may build reputation and start behaving maliciously. But this paper assumes that a good node is always honest.

D. Trust Management Architecture (TMA) [7].

A novel hierarchical trust management scheme that minimizes communication and storage overheads is proposed by the authors. This scheme considers both direct and indirect trust in trust evaluation. This paper introduces a new node called a sponsor node in the network. Sponsor node selects the target nodes based on both trust and energy of the target nodes. The main focus of this paper will be to develop a formal model for modeling trust in hierarchical ad hoc sensor networks to enable mobile sensor nodes to form, maintain, and exchange trust opinions with minimal overheads in terms of complex computations at sensor nodes.

III. PROPOSED SYSTEM

The main drawback of the existing system is that WSN has high computation and storage requirements and if an SN that is on the forwarding path does not forward a packet, and then its next hop neighbor on the forwarding path will identify this event and report the SN as a black hole. This scheme is very expensive for a network within black hole nodes. Therefore, the proposed system Active Detection Routing to Address Black hole deals with the nodal trust and active detection of black hole attacks.

The main features are as follows:

1. The Active Trust scheme is the first routing scheme that uses active detection routing to address BLA. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed
2. The Active Trust route protocol has better energy efficiency. Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes. Therefore, the Active Trust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots. Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security.
3. The Active Trust scheme has better security performance. Compared with previous research, nodal trust can be obtained in Active Trust. The route is created by the following principle. First, choose nodes with high trust to avoid potential attack, and then route along a successful detection route. Through the above approach, the network security can be improved.

A. System Architecture

Figure 3.1 depicts proposed system architecture. In this proposed model consists of three modules namely:

- Initialization phase
- Active trust phase
- Data routing phase

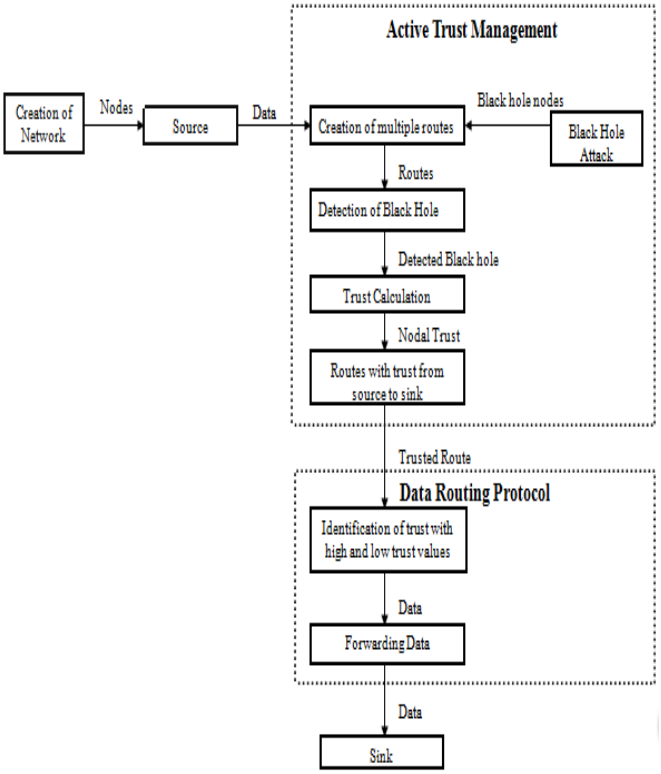

Figure 3.1: System Architecture

1. Active detection routing: 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.
2. 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.
3. Data Routing: The core idea of data routing is that when any node receives a data packet, it selects one node from the set of candidates nearer the sink whose trust is greater than the preset threshold as the next hop. If the node cannot find any such appropriate next hop node, it will send a feedback failure to the upper node, and the upper node will re-calculate the unselected node set and select the node with the largest trust as the next hop; similarly, if it cannot find any such appropriate next hop, it sends a feedback failure to its upper node.
4. Calculation of trust: During data routing and detection routing, every node will perform a nodal trust calculation to aid in black hole avoidance. When node A performs a detection route for node B at time, if the detection data are successfully routed, consider the trust of node A to B to be ; otherwise, consider the trust to be. Considering

that A has interactions with B during , the detection value order by time is as follows:

$$\left\{\Delta_A^B(t_1)\,|\,\Lambda_A^B(t_1),\ \Delta_A^B(t_2)\,|\,\Lambda_A^B(t_2),\ \ldots\ \Delta_A^B(t_w)\,|\,\Lambda_A^B(t_w)\right\}$$

IV. IMPLEMENTATION

The implementation is done in NS2.35 using TCL scripts and C++coding. The pseudo code used for implementation is:

1. Active Trust Algorithm:

Step 1: Source node selects an undetected node to launch the detection route.
Step 2: For each node that receives detection packet maximum route length ω is decreased by 1.
Step 3: If ω = 0, then Generate feedback packet and launch a feedback route to source and restore to initial value
Step 4: If ω≠0, then Continue to select the next hop
Step 5: If ω≠0, then Detection route continues
Step 6: If Detection route is successful-data is routed to destination.

2. Data Routing Algorithm:

Step 1: For each node that generates or receives a data packet, such as node A, Do Select B as the next hop such that B has never been selected in this data routing process, has the largest trust and is nearer the sink
Step 2: If A finds such node, for instance, node B Send data packet P to node B
Step 3: If node B is the sink then, this data routing procession is completed
Step 4: End if
Step 5: Else, Send failure feedback to the upper node, such as node C
Step 6: End if
Step 7: End for
Step 8: For each node that receives failure feedback, such as node B, Do Repeat step 5 to step 9
Step 9: End for

V. RESULT ANALYSIS

To analyze the results in networks, usually throughput, delay, overhead, energy and packet delivery ratio are considered. The proposed scheme gives good results on packet delivery ratio, throughput and energy parameters. The screenshots of the results are shown n below figure 5.1, 5.2, 5.3, 5.4, 5.5, 5.5, and 5.6 respectively.

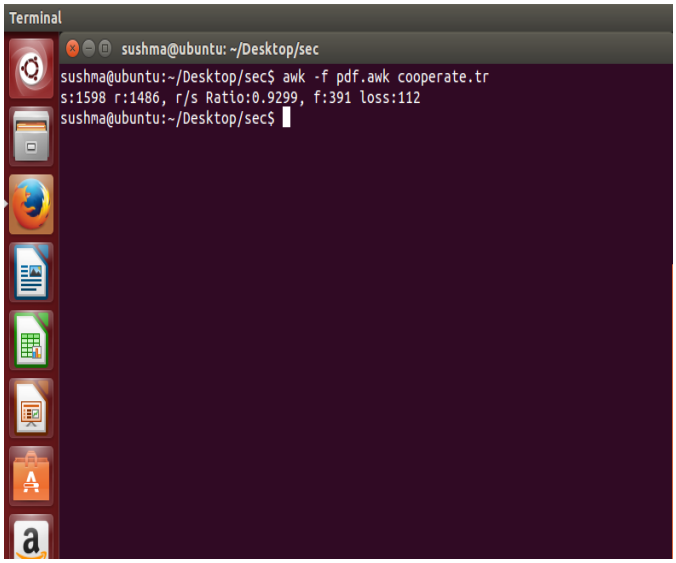

Figure 5.1: packet delivery ratio

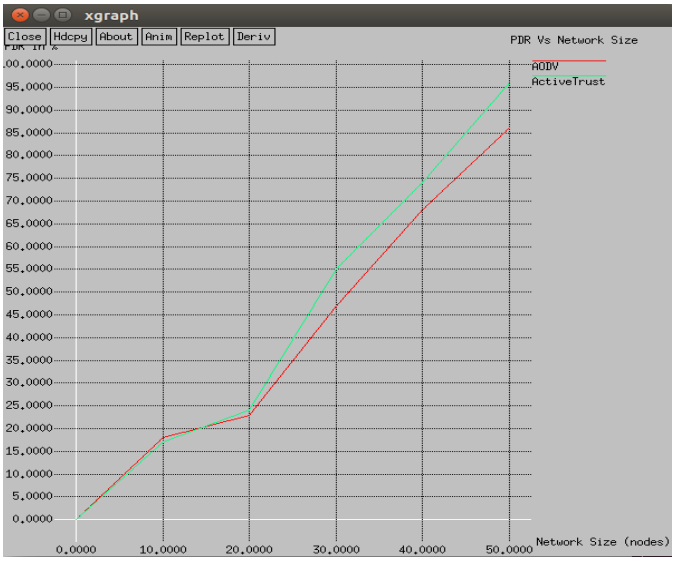

Figure 5.2: packet delivery ratio graph

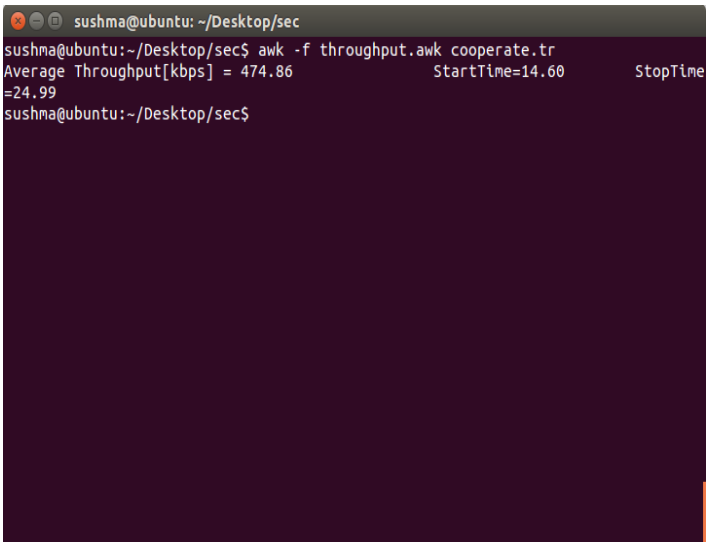

Figure 5.3: throughput

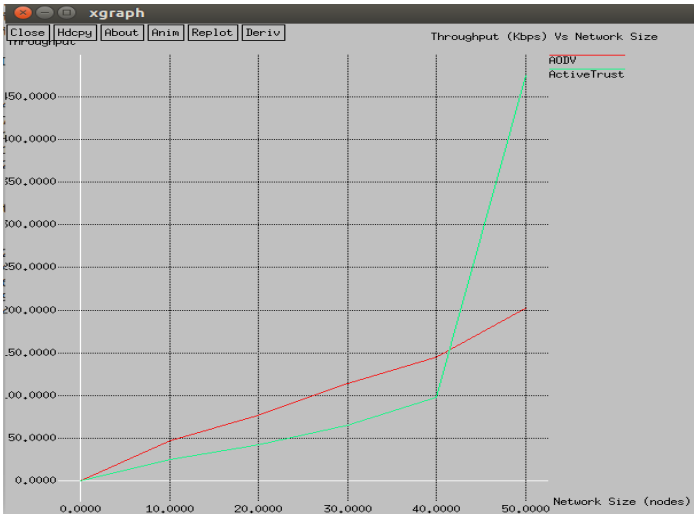

Figure 5.4: throughput graph

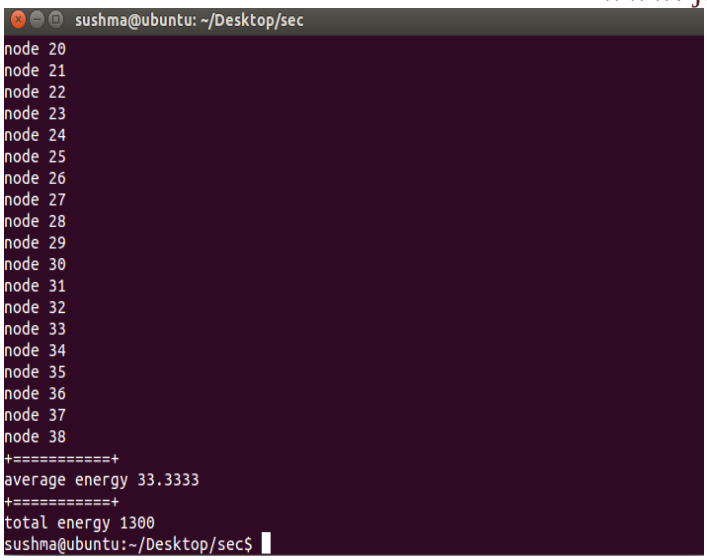

Figure 5.5: Energy

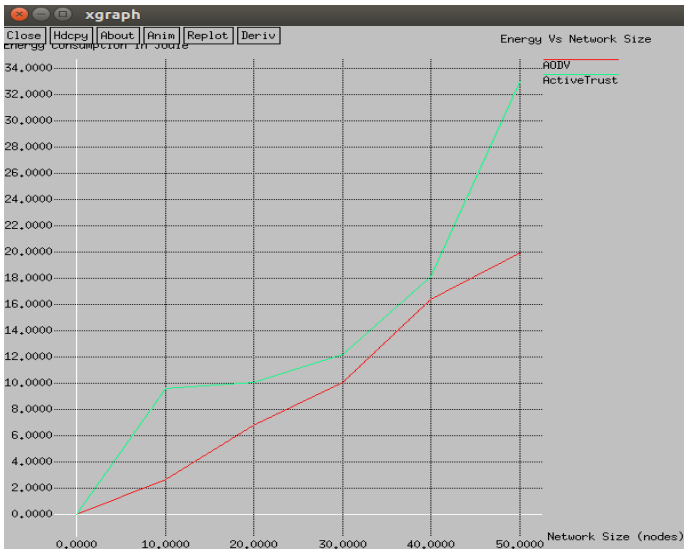

Figure 5.6: Energy graph

CONCLUSION

In this paper, 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 successful routing probability.
2. High energy efficiency. The Active Trust scheme fully uses residue energy to construct multiple detection routes. Further, scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

References

[1] Qinghua Wang and Ilangko Balasingham, "Wireless sensor networks - an introduction"

[2] G. Padmavathi and D.Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," volume 4, pages 1 - 9, International Journal of Computer Science and Information Security, 2009.

[3] Sakshi Srivastava and Kushal Johari, " A survey on reputation and trust management in wireless sensor network," volume 1, pages 139 - 149, International Journal of Scientific Research Engineering Technology, August 2012.

[4] Ke Liu, Nael Abughazaleh and Kyoung Donkang., "Location verification and trust management for resilient geographic routing," ELSEVIER, 2007.

[5] Efthimia Aivaloglou and Stefanos Gritzalis, "Hybrid trust and reputation management for sensor networks," Springer, October 2009.

[6] Riaz Ahmed Shaikh, Hassan Jameel, Brian J d Auriol, Heejo Lee, Sungyoung Lee, and Young- Jae Song, "Group-based trust management scheme for clustered wireless sensor networks," pages 1698 - 1712, IEEE Transactions on Parallel and Distributed Systems, October 2009. Reshmi . V et al. / International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 5 No. 02 Feb 2014 108

[7] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan, and Abdul Sattar, "A trust management architecture for hierarchical wireless sensor networks," pages 268 - 271, IEEE Conference, 2010.