An Active Trust: Secure and Trustable Routing in Wireless Sensor Networks

Kavya KG
M.Tech Student
VIAT Muddenahalli

Dr. Sarika Tale
Associate Prof & HOD
Dept of DECS
VIAT Muddenahalli

***Abstract*— Wireless sensor networks [WSNs] are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. To conquer that challenge, an active detection-based security and trust routing scheme named Active Trust is proposed for WSNs. The most important innovation of Active Trust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. It is assailable to attacks like black hole and gray hole. In a black hole attack a malicious node act like ordinary node, but if a data packet passes through malicious node it consumes data packet and never forward it to neighboring nodes, whereas in a gray hole attack the malicious node will forward the data packet with selective data. Here we are presenting a defense mechanism for detection of cooperative black hole attack by multiple black hole nodes and the prevention of attack in multiple base stations. The simulation carried out on the proposed mechanism has produced results that elaborate the detection mechanism against the attack while maintaining a level of throughput in Manets**

Keywords*- *Security Trust, Blackhole Attack, Wsn

I. INTRODUCTION

Wireless Sensor Networks [WSNs] are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of novel attacks . A black hole attack [BLA] is one of the most typical attacks. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security in WSNs. There is much research on black hole attacks. Such studies mainly focus on the strategy of avoiding black holes. Another approach does not require black hole information in advance. In this approach, the packet is divided into M shares, which are sent to the sink via different routes [multi-path], but the packet can be resumed with T shares [T<=M]. However, a deficiency is that the sink may receive more than the required T shares, thus leading to high energy consumption; Another preferred strategy that can improve route success probability is the trust route strategy. There is much related research, such as. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully; thus, routes created in this manner can forward data to the sink with a higher success probability . However, the current trust-based route strategies face some challenging issues. [1] The core of a trust route lies in obtaining trust. However, obtaining the trust of a node is very difficult, and how it can be done is still unclear. [2] Energy efficiency. Because energy is very limited in WSNs, in most research, the trust acquisition and diffusion have high energy consumption, which seriously affects the network lifetime. [3] Security. Because it is difficult to locate malicious nodes, the security route is still a challenging issue. Thus, there are still issues worthy of further study. Security and trust routing through an active detection route protocol is proposed in this paper. The main innovations 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. In this way, the attacker's behavior and location, as well as nodal trust, can be obtained and used to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs [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. However, we find it possible after carefully analyzing the energy consumption in WSNs. Research has noted that there is still up to 90% residue energy in WSNs when the network has died due to the "energy hole" phenomenon. Therefore, the Active Trust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots [to improve network lifetime]. Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security. According to theoretical analysis and experimental results, the energy efficiency of the Active Trust scheme is improved more than 2 times compared to previous routing schemes, including shortest routing, multi-path routing. [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. [4] Through our extensive theoretical analysis and simulation study, the Active Trust routing scheme proposed in this paper can improve the success routing probability by 1.5 times to 6 times and the energy efficiency by more than 2 times compared with that of previous researches In a MANET, security of routing protocol is critical problem. More than one node can be compromised in a MANET such a way that they act like a malicious node so detection of these nodes will not be easy. These nodes may generate false data or drop the data packet. These nodes also have the ability to change the path of data packets. These nodes also generate message to non-existence links or provide incorrect link state information. MANET uses ad hoc on-demand distance vector [AODV] routing protocol. It is source initiated on demand routing protocol. AODV is prone to black hole attack The authors have proposed that black hole nodes in a MANET work independently and proposed an algorithm to prevent a single black hole, but the proposed algorithm does not work in case of cooperative black hole attack.

II. THE SYSTEM MODEL AND PROBLEM STATEMENT

A. The System Model

[1] Network model

[a] We consider a wireless sensor network consisting of sensor nodes that are uniformly and randomly scattered in a circular network; the network radius is R , with nodal density ρ , and nodes do not move after being deployed . Upon detection of an event, a sensor node will generate messages, and those messages must be sent to the sink node. [b] We consider that link-level security has been established through a common cryptography-based protocol. Thus, we consider a link key to be safe unless the adversary physically compromises either side of the link. [2] The adversaries model We consider that black holes are formed by the compromised nodes and will unselectively discard all packets passed by to prevent data from being sent to the sink . The adversary has the ability to compromise some of the nodes. However, we consider the adversary to be unable to compromise the sink and its neighboring nodes .

B. Energy Consumption Model and Related Definitions

According to the typical energy consumption model Eq. [1] represents energy consumption for transmitting, and Eq. [2] represents energy consumption for receiving. Eelec represents the transmitting circuit loss. Both the free space [2d power loss] and the multi-path fading [4d power loss] channel models are used in the model depending on the distance between the transmitter and receiver. fs ε and amp ε are the respective energy required by power amplification in the two models

C. Problem Statement

[1] Network lifetime maximization. Network lifetime can be defined as the first node die time in the network. For Ei as the energy consumption for node i, the lifetime maximization can be expressed as the following: max[T] min max[Ei]

[2] The data collection has better security performance and strong capability against black hole attacks. The main goal of our scheme is to ensure that the nodal data safely reach the sink and are not blocked by the black hole. Thus, the scheme design goal is to maximize the ratio of packets successfully reaching the sink. Consider that the number of packets that are required to reach the sink is M and that the number of packets that ultimately succeed in reaching the sink is m ; the success ratio is q = m/M Our goal is to maximize the success ratio, that is, max[q] .

MANET is the most successful and widely used network today, as there is no need of any infrastructure to exchange message with one another or from one device to another device. There are three kinds of routing protocols over which the MANET works. They are reactive protocols, proactive protocols and hybrid protocols. The basic difference between these protocols is that in reactive protocol the route is discovered whenever it is demanded by a node and in proactive protocols, they have the information about the destinations in the network. Hybrid protocol carries the functionality of both the reactive and proactive protocols. MANET is in high demand today but it also has many security issues. It is vulnerable to many attacks like wormhole attack, denial of service, eavesdropping etc. Black Hole Attack is one of the major attack to which MANET is vulnerable. In this attack, a node presents itself as it has the shortest path to convey the message to the desired node and thus the source node starts sending the packets to the destination node via that node. But as it was the malicious node, it instead of sending the packets further in the network starts dropping them and thus compromises the security. Much of the work has been done before by other writers over Black Hole attack in MANET using different procedures. Some made use of digital signature; some introduced a new node in the network. In this thesis, the detection of malicious node will be carried out by using a table in the network.

III. ACTIVE TRUST SCHEME DESIGN

A. Overview of the Proposed Scheme

An overview of the Active Trust scheme, which is composed of an active detection routing protocol and data routing protocol, is shown in below .

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.

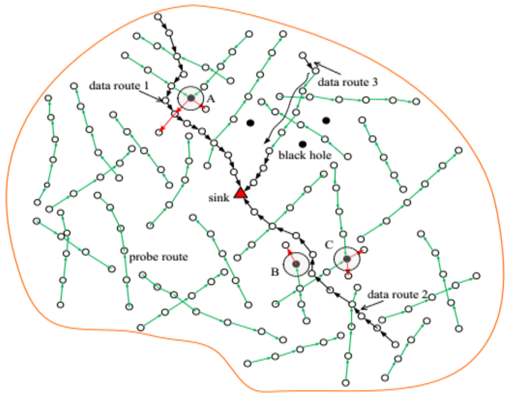


Fig. 1: Illustration of the ActiveTrust scheme

The simulation tool used for this study is Ns-2. Ns-2 is one of the discrete-event network simulator used in research and training. Ns-2 works at packet level and also provides considerable support to simulate many protocols like DSR, TCP, FTP, UDP and HTTP. It simulated both wired and wireless networks. It is primarily UNIX based and its scripting language is TCL. Ns-2 is said to be standard experiment environment in research community. It is a discrete event scheduler. The goals of ns-2 are to support networking research and education like protocol design, traffic studies etc. It also supports protocol comparison, new architecture designs. It provides collaborative environment. Scripts are written in TCL language. TCL is the short form of Tool Command Language. It is a programming language which is very dynamic. It is widely used in desktop and web applications, testing, networking etc. It is highly extensible and easily deployed. TCL language is compatible with C language and the libraries of TCL can be easily operated in C language. This is the most significant feature of TCL language.

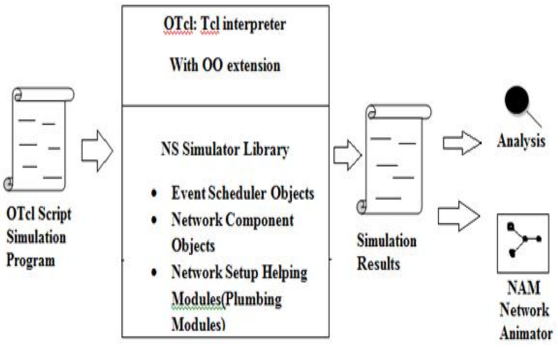

OTcl: Tcl interpreter
With OO extension
NS Simulator Library
• Event Scheduler Objects
• Network Component Objects
• Network Setup Helping Modules(Plumbing Modules)
OTcl Script Simulation Program
Simulation Results
Analysis
NAM Network Animator

Fig 2: Network Simulator Tool

B. Active Detection Routing Protocol

Algorithm 1: Active Detection Routing Protocol

```
Initialization
For each neighbor node An Do
    Let An access Time=Current time
End for
For each node that generates a detection packet, such as node A, Do
    Construct packet P, and do value assignment for $\omega$ and $\varpi$
    Select B as the next hop which B meets access time is the minimum and nearer the sink //B is the node that is the longest time undetected and nearer the sink
    Send packet P to node B
End for
For each node that receives a detection packet, such as node B, Do
    let $P.\omega = P.\omega - 1$, $P.\varpi = P.\varpi - 1$
    If $\varpi = 0$ then
        Construct feedback packet q, and do value assignment for each part
        Send feedback packet q to the source
    End if
    If $p.\omega \neq 0$ then
        detection routing continue
    End if
End for
For each node that receives feedback packet q, such as node C, Do
    If q destination is not itself then
        send q to the source node
    End if
End for
```

c. Data Routing Protocol

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. The protocol is as follows:

Algorithm 2: Data Routing Protocol

```
For each node that generates or receives a data packet, such as node
    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
```

```
4: If A finds such node, for instance, node B
5: Send data packet P to node B
6: If node B is the sink then
 7: this data routing procession is completed
 8: End if
9 :  Else
10: Send failure feedback to the upper node, such as node C
11: End if
12: End for
13:For each node that receives failure feedback, such as node B, Do
14: Repeat step 2 to step 11
15: End for
```

D. BLACK HOLE ATTACK

In this assault, the noxious Node promote itself to have the most limited course for the correspondence and exchanging of bundles, and in this manner drops the parcels without sending them to the neighboring Nodes. Black hole attack is one of the conceivable assault and almost normal assault in WSN. It can be said as the Denial of Service. In this assault, a node produces a RREQ message and passes it to its neighbors; a malicious node publicizes that it has the best way to the goal hub amid the procedure of course disclosure. When it gets the RREQ message from source node, it promptly sends back a fake RREP message towards it. The source node gets the RREP message and begins sending the parcel to it. At the point when source node begins sending bundles to the goal by utilizing this course, the vindictive node drops all parcels as opposed to sending it. At the end of the day one might say that it "swallows" the information packet .

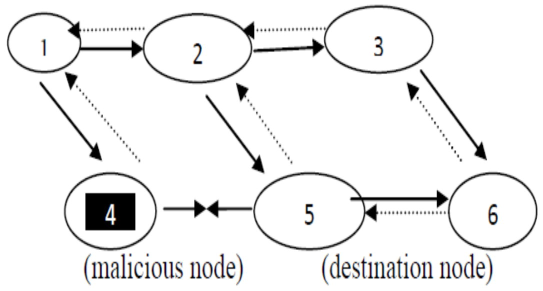


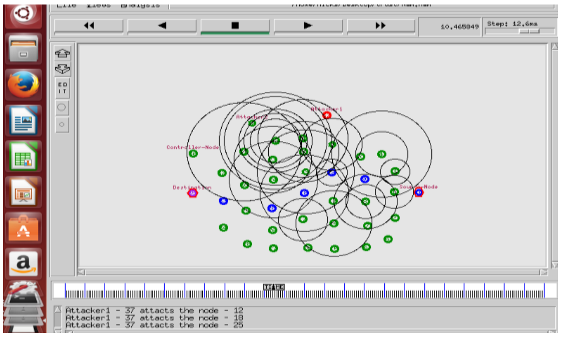
Fig 3: Black hole attack in WSN

In the above figure, there are 6 nodes out of which node 1 is the source node which creates the RREQ message keeping in mind the end goal to locate the new course to send a parcel to the goal node i.e. node 6. The transitional nodes of node1 are node 2 and node 4. Both the nodes get the RREQ message created by the node1. node 4, being the malignant node, sends the RREP message back to the node1 promoting that it has the best way to the goal node, node6. Subsequent to getting the RREP message from node 4, node 1 began sending the parcel to the node 4. However, node 4 won't forward it; it disposes of the considerable number of messages simply making it the refusal of administration

IV. EXPERIMENTAL RESULTS

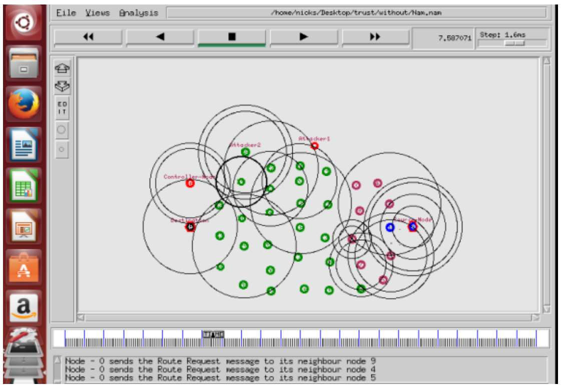
The result stage or phase of project or plan is where system is evaluated or calculated in terms of performance or output and verified if the goals that are stated in the beginning are met. The aim at this point is to get the required data which is plotted for checking against performance. We can calculate the value of Overhead Throughput, Delay, PDR using graph in UBUNTU Software

A.SIMULATION USING NS-2 FOR ALERT PROTOCOL



```
Attacker1 - 37 attacts the node - 12
Attacker1 - 37 attacts the node - 18
Attacker1 - 37 attacts the node - 25
```

Fig 4: With malicious node



```
Node - 0 sends the Route Request message to its neighbour node 9
Node - 0 sends the Route Request message to its neighbour node 4
Node - 0 sends the Route Request message to its neighbour node 5
```

Fig 5: without malicious node

V. CONCLUSION

From the outcomes we've come to comprehend that novel security and trust routing subject upheld dynamic location, has the resulting heavenly properties: [1] High famous directing possibility, security and evaluate capacity. The trust subject will rapidly locate the nodal trust thus avoid suspicious nodes to rapidly convey the products a very nearly 100 percent prominent directing shot. [2] High vitality intensity, to develop different identification courses trust subject uses completely. The hypothetical examination and test comes about have demonstrated that our topic enhances the famous routing chance by more than three times, up to ten times now and again. Further, our project enhances each the vitality power and in this way the system security performance .and recognizes both dark and dim gap assault and it has essential criticalness for remote detecting component arrange security. In future by exploitation cryptanalytic procedure a ton of data will be secure as like trust secure and trustable directing in WSN and conjointly clone detection will be finished.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to prof. Dr. Sarika Tale [HOD], Department of Digital Electronic and Communication Systems, Visvesvaraya Institute of Advanced Technology. who gave me the golden opportunity to do this wonderful project on the topic [An Active Trust: Secure And Trustable Routing In Wireless Sensor Networks], which also helped me in doing a lot of research and I came to know about so many new things we are really thankful to them. And, secondly I would also like to thank my parents and friends who helped me a lot in finalizing this project within the limited time frame.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[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] Y. Hu, A. Liu. "An efficient heuristic subtraction deployment strategy to guarantee quality of event detection for WSNs," The Computer Journal, vol. 58, no. 8, pp. 1747-1762, 2015.

[7] 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.

[8] 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.

[9] 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.

[10] JianWang,YanhengLiu,Yu Jiao “Efficient routing algorithm for wireless sensor network”,IEEE transactions on sensors , vol13

[11] 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.

[12] Y. L. Yu, K. Q. Li, W. L. Zhou, P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880, 2012.

[13] S. J. Lee, M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," IEEE ICC, pp. 3201-3205, 2011.

[14] T. Shu, M. Kurtz, 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.

[15] 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.

[16] [16]. T. P. Nghiem, T. H. Cho, "A multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks," Computer Communications, vol. 33, no. 10, pp. 1202-1209, 2010.

[17] Q. He, D. Wu, P. K. Sori, "a secure and objective reputation-based incentive scheme for ad hoc networks," IEEE Wireless Communications and Networking Conference, pp. 825–830, 2004

[18] S. Kamvar, M. Schlosser, H. Garcia-Molina, "The eigen trust algorithm for reputation management in P2P networks," in: Proceedings of the 12th International Conference on World Wide Web, pp. 640–651, 2003.