ACTIVETRUST: SECURE AND TRUSTABLE ROUTING IN WSN

Meera C, RaviKumaran P

Department of computer science& Engg, Fatima Michael college of Engg & Tech, Anna University, Madurai
meerachokkalingam5@gmail.com
Head of the department, Department of computer science& Engg, Fatima Michael college of Engg & Tech, Anna University, Madurai

Abstract—The Security and trust routing through an active detection data route protocol (ADDRP) in which unique path key is established for all sensors in the path. The ActiveTrust scheme is the first routing scheme that uses active detection routing to address black hole attack (BLA). The most significant difference between ActiveTrust 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. It avoids block hole attackers through the active creation of a number of detection routes to quickly detect and obtain node security and thus improves the data route security. The ActiveTrust route protocol has better energy efficiency. Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. The ActiveTrust scheme has better security performance and optimize network lifetime.

Keywords- Active detection data route protocol, Active Trust, Black hoe attack.

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 [1]. 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 [2][3]. A black hole attack (BLA) is one of the most typical attacks [4] and works as follows. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to forwarded to the sink because making decision is the incorrect and fails[5].How to detect and avoid BLA is of great significance for security in WSNs and another approach he 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*). Thus leading to energy consumption; Another preferred strategy that can improve route success probability is the trust route strategy. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully. Security and trust routing through an active detection route protocol is proposed in this paper. The main innovations are as follows. (1) The ActiveTrust scheme is the routing scheme that uses active detection routing to address BLA. (2) This ActiveTrust route protocol has better energy efficienc upto 90%. (3)It has better security performance, trust can be obtained by ActiveTrust. First, choose nodes with high trust to avoid potential attack, and then route along a successful etection route. Through the above approach, the network security can be improved. The ActiveTrust 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.

II RELATED WORK

Single-path routing is a simple routing protocol [6] but is easily blocked by the attacker. Therefore, the most natural approach is via multi-path routing to the sink. Even if there is an attack in some route, the data can still safely reach the sink [4]. Multi-path routing protocols can be classified into two classes depending on whether the data packet is divided. One is multi-path routing without share division. The other is multi-path routing with share division, i.e., the packet is divided into shares, and different shares reach the destination via different routes[4].(1) Non-share-based multi-path routing. There are different multi-path route construction methods. Reference proposes a multi dataflow topologies (MDT) approach is the selective forwarding attack. In the MDT approach,the network is divided into two dataflow topologies. Even if one topology has a malicious node, the sink can still obtain packets from the other topology. (2) Share-based multi-path routing protocols. The SPREAD algorithm in is a typical share-based multi-path routing protocol. The basic idea of the SPREAD algorithm is to transform a secret message into multiple shares, which is called a (*T*, *M*) threshold secret sharing scheme . Its are delivered by multiple independent paths to the sink such that, even if a small number of shares are dropped, the secret message as a whole can still be recovered. The advantage of this algorithm is that through multi-path routing, each path routes only one share, and the attacker must capture at least *T* shares to restore nodal information, which increases the attack difficulty [5]. Thus, the privacy and security can be improved. In the above research, the multi-path routing algorithms are deterministic such that the set of route paths is predefined under the same network topology. This weakness opens the door for various attacks if the routing algorithm is obtained by the adversary.

III Proposed Work

Proposed a Active Detection Data Routing Protocol (ADDRP) in this process. The Active Detection protocol algorithm is used to find the neighbore node of in this network. Calculation of Nodal Trust Algorithm - During data routing and detection routing, every node will perform a nodal trust calculation to aid in black hole avoidance. These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers.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.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. 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. 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.

- Network formation and Neighbor discovery
- Misbehavior Detection
- Trust value calculation and performance.

A) Network formation and Neighbor discovery

To create the node in the particular region and decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly. Network of 25 nodes is created using network simulator for wireless ad-hoc network. Encryption decryption is done by RSA Algorithm.Detection of misbehavior nodes using Security Packet, then send communication between source to destination node.RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. If the authentication is successful then it sends data packet through the Reliable routing path.RSA provides end-to-end confidentiality and hop-by-hop authentication.

On-demand reactive routing protocol that uses routing tables with one entry per destination. When a source node needs to find a route to a destination, it starts a route discovery process, based on flooding, to locate the destination node. Upon receiving a route request (RREQ) packet, intermediate nodes update their routing tables for a reverse route to the source. Similarly, the forward route to the destination is updated upon reception of a route reply (RREP) packet originated either by the destination itself or any other intermediate node that has a current route to the destination.

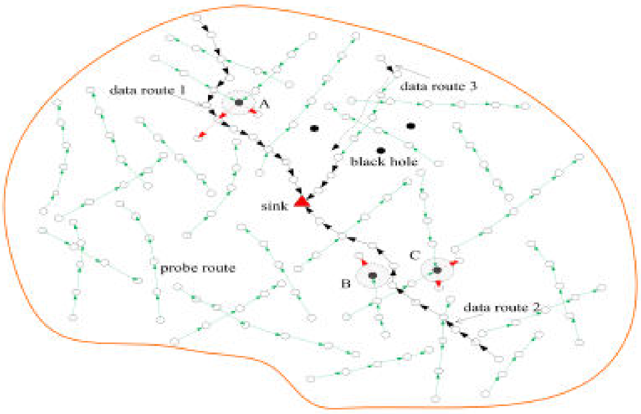

Fig. 1. Finding active route for data transmission.

The clustering formation is depend upon the Position of the each nodes in the WSNs. The cluster Head is depend upon the Energy of the nodes in the clustering. The deputy cluster head (DCH) is used, which increases the lifetime of the network.The value of position, velocity, speed and energy are maintained and updated at the base station. Each Cluster Head send communication via the base station.Base station monitor the each and every nodes in WSNs and All the nodes details are updated in the BS.

B)Misbehavior Detection :

Route discovery for shortest and freshest path.When a source node needs to find a route to a destination, it starts a route discovery process, based on flooding, to locate the destination node. Upon receiving a route request (RREQ) packet, intermediate nodes update their routing tables for a reverse route to the source. After reaches the destination node- Sends Route reply packets to source node.Transmit the data from source node to destination node through energy efficient intermediate nodes, If any path failure occurs again starts route discovery.Route request send to all intermediate nodes between source S and destination D.Route discovery for shortest and freshest path using ADDRP. Check the Neighbor list.Detection of misbehavior nodes using Security Packet then send communication between source to destination node.

Identity Collection:

The first phase gathers participatingneighbors, ensuring that no conforming identities are jammed by attackers. The initiator sends a REQUEST message stating its identity, e.g., a public key. All stationary neighbors respond with their identities via HELLO-I messages, each ACKed by the initiator. Unacknowledged HELLO-Is are re-transmitted. The process terminates when the channel is idle—indicating all HELLO-I's were received and ACKed. If the channel does not go idle before a timeout (e.g., 15 seconds), the protocol aborts because an attacker may be selectively jamming some HELLO-Is. The protocol also aborts if too many identities join, e.g., 400.

Randomized Broadcast Request:

The second phase is the challenge-response protocol to collect RSSI observations for motion detection and Sybil classification. First, each identity contributes a (difficult to predict) random value; all are hashed together to produce a seed to generate the random sequence of broadcast requests issued by the initiator. Specifically, it sends a TRANSMIT message to each participant in the random sequence, who must quickly broadcast a signed HELLO-II, e.g., within 10 ms in our implementation.12 Each participant records the RSSIs of the HELLO-II messages it hears. Some identities will not hear each other; this is acceptable because the initiator needs observations from only three other conforming identities. |I| X s requests are issued, where s is large enough to ensure a short minimum duration between consecutive requests for any two pairs of nodes, e.g., 14 in our tests. An identity that fails to respond in time might be an attacker attempting to change physical position and is rejected. In some applications, it might be desirable to meet the additional requirement that attackers be unaware of their positions in the challenge-response sequence until challenged. This could be achieved by allowing the initiator to use a self-generated random sequence that cannot be verified by other participants.

C) Trust value calculation and Performance:

This method calculate the Trust value on basis of three parameters.

- Energy
- Packet count.
- Queue Size.

Trust calculation:

$$T_c = t_s + P / 2$$

where,

T_c - Trust calculation

t_s - Time success

P - Positive real number

T - Time transcation.

```
if (T_CV > 0.7)

Begin,

    Malicious node is detected
    add to block list

else

   Data transmitted

End
```

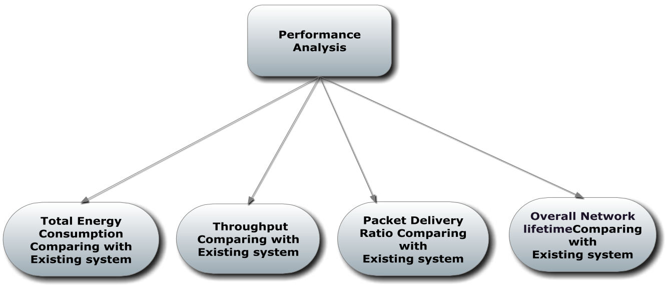
Performance Analysis
Total Energy Consumption Comparing with Existing system
Throughput Comparing with Existing system
Packet Delivery Ratio Comparing with Existing system
Overall Network lifetimeComparing with Existing system

Fig. 2. Performance Analysis

Throughput = No of Packets Received/ Simulation Time

Delay = No of packets Sent / Simulation Time

Delivery Ratio = No of packets Received/ No of Packets sent

Packet transmission time = Packet size / Bit rate

$$CE =(\sum_{i}^{n} \text{Initial\_Energy} - \text{Final\_Energy [i]})^{n}$$

where,

CE - Consumed Energy

i - Initially i is 0

n - number of nodes

Total Energy:

TE + = CE[i]

ALGORITHM

```
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 nearer the sink.
    If A finds such node, for instance, node B
        send data packet P to node B
        If node B is the sink then
            This data routing process is completed.
        End if
    Else
        send failure feedback to the upper node, such as node C
    End if
End for
```

IV EXPERIMENTAL RESULT

In our simulation-based evaluation, we solely focus on the data packets transfer in the trustable route. For each topology we determine the neighbor sets of all nodes and link qualities. The probability of successful routing of ActiveTrust scheme for different BLA. Packet is not dropped due to black hole attack or denial of service attack. The result is that the throughput of network is much better than that of energy efficiency and security.

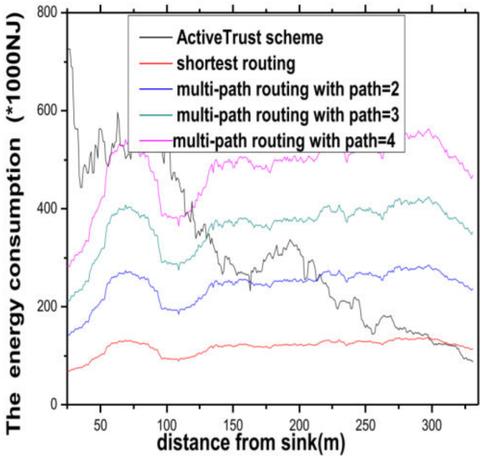

Fig 3:Energy consumption under different scheme

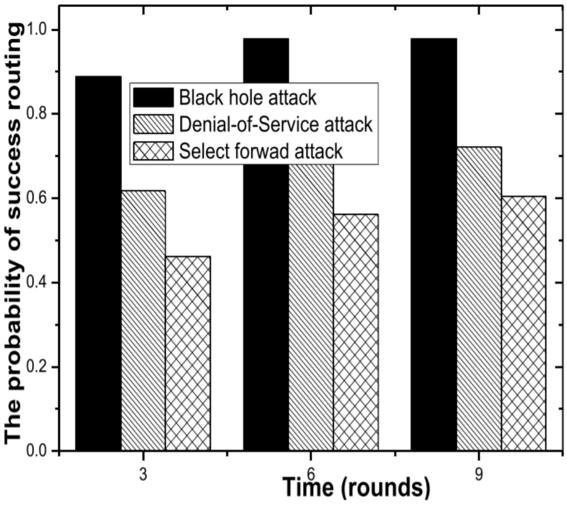

Fig 4 :The probability of successful routing for different BLAs

V CONCLUSION

High successful routing probability, security and scalability. The ActiveTrust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. High energy efficiency. The ActiveTrust 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 case.

VIFURTURE WORK

Further, Our scheme improves both the energy efficiency and the network security performance. It will have significant improtant in wireless sensor networks.

VII REFERENCE

[1] Y. Hu, M. Dong, K. Ota, A. Liu, and M. Guo, “Mobile target detection in wireless sensor networks with adjustable sensing frequency,” IEEE Syst. J., to be published, doi: 10.1109/JSYST.2014.2308391.

[2] A. Liu, M. Dong, K. Ota, and J. Long, “PHACK: An efficient scheme for selective forwarding attack detection in WSNs,” Sensors, vol. 15, no. 12, pp. 30942–30963, 2015.

[3] A. Liu, X. Jin, G. Cui, and Z. Chen, “Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network,” Inf. Sci., vol. 230, pp. 197–226, May 2013.

[4] T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sensor networks using randomized dispersive routes,” IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010

[5] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for WSNs," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 613–625, Mar. 2015.

[6] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, "Differential game-based strategies for preventing malware propagation in wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. 9, no. 11, pp. 1962–1973, Nov. 2014.

[7] O. Souihli, M. Frikha, and M. B. Hamouda, "Load-balancing in MANET shortest-path routing protocols," Ad Hoc Netw., vol. 7, no. 2, pp. 431–442, 2009.

[8] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," J. Parallel Distrib. Comput., vols. 81–82, pp. 47–65, Jul. 2015.

[9] S. He, J. Chen, X. Li, X. Shen, and Y. Sun, "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE Trans. Mobile Comput., vol. 13, no. 6, pp. 1268–1282, Jun. 2015.

[10] S. H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 371–383, Feb. 2015.

[11] Y. Hu and A. Liu, "An efficient heuristic subtraction deployment strategy to guarantee quality of event detection for WSNs," Comput. J., vol. 58, no. 8, pp. 1747–1762, 2015.

[12] S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in Proc. IEEE ICC, Jun. 2011, pp. 3201–3205.

[13] Y. Zhang, S. He, and J. Chen, "Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks," IEEE/ACM Trans. Netw., to be published, doi:10.1109/TNET.2015.2425146.