Enhancing the Network Lifetime in Wireless Sensor Networks by Using Trust Based Secure Routing Protocol

***P.Amrutha*[1], *Dr.N.Geethanjali*[2], *Dr.N.Ramesh Babu*[3], *V. Subhashini*[4]**
[1]*Research Scholar, Department of Computer Science and Technology,*
Sri Krishna Devaraya University, Ananthapuramu, Andhra Pradesh, India.
p.amruthachowdary@gmail.com
[2]*Professor, Department of Computer Science and Technology,*
Sri Krishna Devaraya University, Ananthapuramu, Andhra Pradesh, India.
geethanjali.sku@gmail.com
[3]*Assitant Professor Department of Computer applications,*
MITS Madanapalle, Chittor, Andhra Pradesh, India.
ramesh.phd.sku@gmail.com
[4]*Research Scholar, Department of Computer Science and Technology,*
Sri Krishna Devaraya University, Ananthapuramu, Andhra Pradesh, India.
subhashinivardhan@gmail.com

Abstract:

In many security applications, Wireless Sensor Networks (WSN) plays vital role. Because of their characteristics such as resilience, scalability and ability to inherent various security attacks. Among the network security attacks, black hole attack is a serious problem this affects the data collection by dropping the sensitive packets and life time of the network by consuming more energy. To beat that challenge, Trust Based Secure Routing Protocol is proposed for WSN's which abstract secure routing by using trust. The novelty of scheme is 1. It avoids the black holes through security detection and 2. It improves the data rates through trust routing. The protocol uses the energy to deduct routes and deduct trust but have the ability to improve the lifetime of a network.

Key words: Wireless Sensor Networks (WSN), Black Hole, Routing, Trust.

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes known as wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to observe physical or environmental conditions, such as temperature, pressure, sound etc. and to supportively pass their data through the network to a main location. A lot of modern networks are bi-directional, also enabling control of detector activity. The development of wireless detector networks was impelled by military applications such as battlefield surveillance; nowadays such networks are utilized in several industrial and consumer applications, such as industrial process observation and control, machine health observation, and so on. Wireless Sensor Networks (WSNs) to shown in figure.1 they are emerging as a promising technology as a result of their wide range of applications in industrial, environmental observation, military and civilian domains. Because of economic concerns, the nodes are sometimes straightforward and low price. They are usually unattended, however, and are therefore probably to suffer from different types of novel attacks.

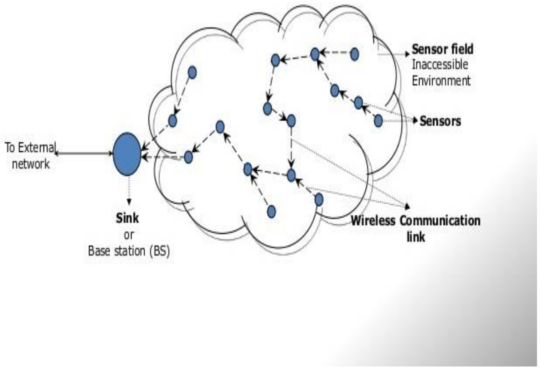

Figure 1: Wireless Sensor Network Architecture

Apart Black Hole Attack (BLA) is one of the most typical attacks and works as follows. The adversary compromises a node and drops all packets that are routed via this node, leading to sensitive data being discarded or unable to be forwarded to the sink. As a result of the network makes decisions depending on the nodes' sensed data; the consequence is that the network can completely fail and, a lot of critically, create incorrect choices. Therefore, however to detect and avoid BLA is of nice significance for security in WSNs.

However, the current trust-based route methods face some challenging problems. The core of a trust route lies in getting trust. However, getting the trust of a node is extremely troublesome, and the way it can be done remains unclear. Energy potency as a result of energy is extremely restricted in WSNs, in most analysis, the trust acquisition and diffusion have high energy consumption, that seriously affects the network lifespan. Security as a result of it is difficult to find malicious nodes; the protection route remains a challenging issue. Thus, there are still issues deserve further study. Security and trust routing through an energetic detection route protocol is projected during this paper. Secure data collection in randomized dispersive routes are Packet is divided into M shares, that are sent to the sink via different routes (multi-path), however the packet are often resumed with T shares by using these traditional system disadvantage is Sink might receive additional than the needed T shares, therefore leading to high energy consumption.

Trust route strategy another preferred strategy that may improve route success chance is that the trust route strategy. the most feature is to form a route by choosing nodes with high trust as a result of such nodes have a higher probability of routing successfully; therefore, routes created during this manner will forward data to the sink with a better success probability, the most aim of this paper is Security and trust routing through secure detection route protocol is projected. trust scheme takes full advantage of the residue energy to produce detection routes and attempts to decrease energy consumption in hotspots. Those observation routes will detect the nodal trust without decreasing lifespan and therefore improve the network security.

The Trust scheme has better security performance. Compared with previous research, nodal trust can be obtained. 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. Through our extensive theoretical analysis and simulation study, the Trust routing scheme proposed in this paper can improve the success routing probability and the energy efficiency.

II. RELATED WORK

Non-share-based multi-path routing there are different multi-path route construction strategies [6]. Proposes a multi dataflow topologies (MDT) approach to resist the selective forwarding attack within the MDT approach, the Network is divided into two dataflow topologies. Even though one topology includes a malicious node, the sink will still acquire packets from the other topology. In such protocols, the deficiency is that if the packet is routed via n routes at the same time, the energy consumption are n times that of one path route, which is able to seriously affect the network lifetime; similar analysis can be seen in multi-path DSR.

Share-based multi-path routing protocols the SPREAD algorithm [8] in may be a typical share-based multi-path routing protocol. The essential idea of the spread algorithm is to transform a secret message into multiple shares, that is termed a (T, M) threshold secret sharing scheme [10]. The M shares are delivered by multiple independent methods to the sink such that, even if a small number of shares are dropped, the secret message as a whole will still be recovered[2,4,10]. The advantage of this algorithm is that through multi-path routing, every path routes only one share, and the attacker should capture a minimum of T shares to restore nodal data, which increases the attack issue. Thus, the privacy and security will be improved. within the above analysis, the multi-path routing algorithms are deterministic such that the set of route paths is predefined under the same network topology[2]. This weakness opens the door for numerous attacks if the routing algorithm is obtained by the individual [9]. For the weakness mentioned on top of, Ref [11]. planned four random propagation strategies: Directed Random Propagation (DRP), Random Propagation (PRP), non-repetitive random propagation (NRRP), and Multicast Tree assisted Random Propagation (MTRP). The overall strategy is as follows. First, divide the message into M shares, and the route path of every share is not planned. Thus, even though the individual acquires the routing algorithm, it is tough to launch a pinpointed node-compromise or jamming attack. As a result of it is difficult to capture over T shares, the security is additionally improved.

In multi-to-one data collection WSNs, we tend to argue that for classic "slicing and assembling" or multi-path routing techniques, sliced shares can merge within the same path with high chance, and this path will be simply attacked by black holes[4]. Thus, in a Security- and Energy-efficient Disjoint Route (SEDR) theme is planned to route sliced shares to the sink with randomized disjoint multipath routes by utilizing the obtainable surplus energy of device nodes. The authors demonstrate that the protection is maximized without reducing the time period within the SEDR protocol. Another methodology to avoid attack and improve route success probability is trust routing. Trust management is becoming a new actuation for finding challenges in ad hoc networks, peer-to-peer networks, and WSNs.

III. PROBLEM STATEMENT

a.Network Model:

We consider the network model consisting of n nodes and the shape of network is randomly deployed. The sender node generates messages and transfers those to sink node. Security among the links and messages are based on cryptography protocol.

b. Adversaries Model:

We consider other network compromises our network nodes and turns into black holes which is dropped the packets or stolen the packets. However we consider the adversaries can't compromise the sink node [2,4].

c. Energy of a Node:

To transfer the packets from sender to the sink need some energy. Thus consumption is as follows

$$E=lE_{ckt}+l€_{amp}d^2$$

Where l is length of packet in bits

E_{ckt} is circuit loss

$€_{amp}$ is energy amplification

D is distance between 2 nodes

d. Distance between Nodes:

Distance from one node to another node is as follows

Consider node1=(x_1,y_1)

node2=(x_2,y_2)

Then $d_x=(x_1-x_2)^2$

$d_y=(y_1-y_2)^2$

So $d_{1,2}=\mathrm{sqrt}(d_x+d_y)$

Where $d_{1,2}$ is distance from node1 to node2.

e. Network Parameters:

Parameter	Symbols	Value
Circuit loss	E_{ckt}	10
Energy amplification	$€_{amp}$	5
Threshold of trust	Θ_t	12
Threshold of energy	Θ_e	10

Table 1: Network Parameters

f. Success Routing:

The data transferred to sink in secure manner against the black hole attacks. So the data is not blocked or dropped by any black hole. Thus, the ratio of packets successfully reached to the sink node is maximized.

Assume number of packets is P which is required to reach the sink node and number of packets p are successfully reached to sink. Then success ratio is as follows,

$$R = p/P$$

The goal is maximize the ratio i.e.,

$$\max(R) = p/P$$

g. Life Time:

One more aim is maximizing the lifetime of network. The die time of first node in the network refers the lifetime of network. To increase the life time of network needs to minimize the maximum energy consumption.

$$\max(T) = \min \max(E_a)$$

Where E_a is energy of node a

h. Trust:

In trust routing scheme, every node calculate the trust of neighbor node to detect black hole. Consider Θ_t is threshold of trust. When node A to B is a detection route at time t_i then trust from node A to B is $\Delta_A^B(t_i)$

Then detection route is routed successfully if $\Delta_A^B(t_i)> \Theta_t$

i.Structure of Packets:

Header	Type	Source	h(hops)	Id

Figure.2: Structure of sending packet

Header	Type	Source	Dest	s-id	Id

Figure.3: Structure of feedback packet

IV. SYSTEM MODEL

An overview of the secure trust scheme, which is composed of routing detection and data transferring, is shown in Figure.4.

a.Routing Detection:

A detection route refers to a route without data packets whose goal is to convince somebody to launch an attack therefore the system will determine the attack behavior and then mark the black hole location. Thus, the system will lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through detection routing, nodal trust can be quickly obtained, and it will effectively guide the data route in choosing nodes with high trust to avoid black holes. The detection protocol is shown via the black line in Figure. 4.

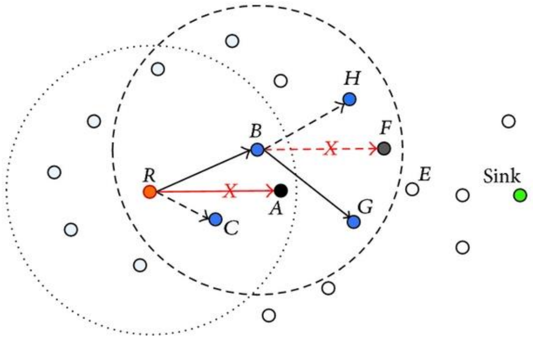

Figure.4: For node *R*, the forwarder list includes nodes *A*, *B*, and *C*. The packet is then transmitted to node B, and node *B* establishes its forwarder list including nodes *H*, *F*, and *G*. A and F are the black nodes

In this scheme, the source node randomly selects an undetected neighbor node to create detection route. Considering that the longest detection route length is, the detection route decreases its length by one for each hop till the length is decreased to zero, so the detection route ends. Data routing protocol refers to the method of nodal data routing to the sink. The routing protocol is comparable to common routing protocols in WSNs the difference is that the route can choose a node with high trust for subsequent hop to avoid black holes and so improve the success ratio of reaching the sink.

The planned system contains the security and trust routing through detection route protocol is planned. Scheme takes full advantage of the residue energy to produce detection routes and attempts to decrease energy consumption in hotspots. Those detection routes can detect the nodal trust without decreasing lifespan and therefore improve the network security. First, select nodes with high trust to avoid potential attack, so route on a successful detection route. Through the higher than approach, the network security is improved. By using this proposed system the following advantages are there initial routing scheme that uses secure detection routing to address BLA, Has better energy efficiency, and has better security performance.

b. Data Transferring:

The core idea of data routing is that once any node receives a data packet, it selects one node from the set of candidates nearer the sink whose trust is greater than the predetermined threshold as the next hop. If the node cannot realize any such acceptable next hop node, it will send a feedback failure to the higher node, and the upper node can re-calculate the random node set and choose the node with the most important trust as the next hop; equally, if it cannot realize any such acceptable next hop, it sends a feedback failure to its higher node. The routing protocol will adopt an existing routing protocol, and that we take the shortest route protocol as an example. Node within the route can select the neighbor that is nearer the sink and has high trust because 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 higher node that there is no path from a to the sink. The upper node, working in the same manner, can re-select a different node from among its neighbors nearer the sink till the data are routed to the sink or there is conclusively no path to the sink.

V. ALGORITHM

```
1.  Initialization
2.  Assign h is number of hops from source to sink
3.  For each node n1 DO
4.     Construct packet p
5.     Select n2 as next node which is nearer to sink
    and have more trust
6.              If n1 finds such a node n2
7.                     Sends packet p to n2.
8.              Else
9.                     Go to step 5
10.             End if
11. End for
12. For node n2 receives packet p DO
13.                 p.h=p.h-1
14.                 If p.h=0 then
15.                       Construct feedback packet f
16.                             Go to step 22
17.                 Else
18.                       Deduction routing continue:
19.                       go to step 3
20.                 End if
21. End for
22. For each node receives feedback packet f, DO
23.                 If f.destination is not itself then
24.                             Send f to source
25.                 End if
26. End for
```

VI. EXPERIMENTAL RESULTS

The experiments adopted number of nodes as 10 among 3 are black holes which generated later. The nodes are deployed random in the network with center of sink node. Initially routing table for 10 nodes is taken. From that network 3 black holes are generated in our work. Randomly one sender is selected, that sends packets to sink via the path which is deducted in routing table. If any node in the path is black hole then that path is avoided and select new path also gives the hint to user that the path exist the black hole. If there is no black hole in the path to sink then the file transferred successfully which had shown in receiver folder in encrypted format.

a.Trust at different nodes:

The number of black hole nodes and good nodes are detected by the trust calculation. Assume Θ_t=12 is threshold of trust. Fig.5 shows trust of different nodes without black hole. Obviously, each node trust in the fig.5 is greater than the threshold. Fig.6 shows trust of different nodes with black hole. The graph clearly shows some nodes trust is less than threshold. So those types of nodes are not detected in routing.

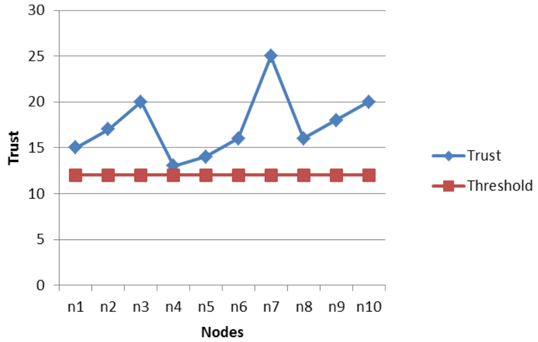

Figure 5 Trust of different nodes without black hole.

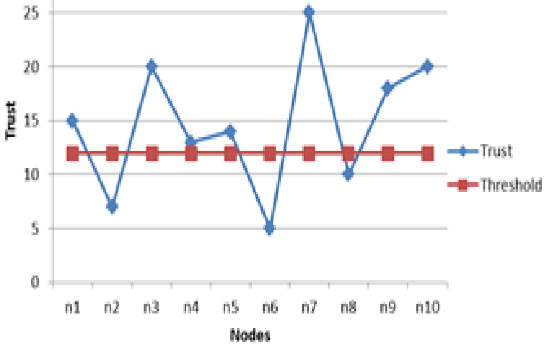

Figure 6 Trust of different nodes with black holes.

b. Trust according to time:

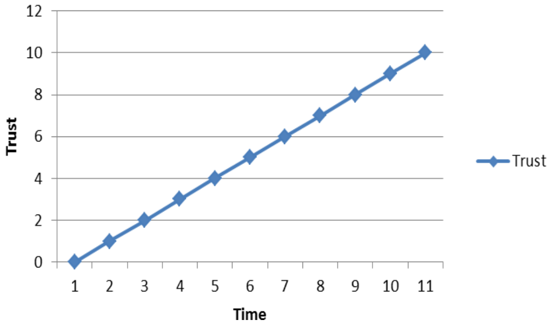

Figure 7 Trust of a good node with respective time.

Assume at the time of zero seconds the trust of nodes is also zero. When the time is increased, the trust value is either increased or decreased with respective good nodes and black hole nodes.

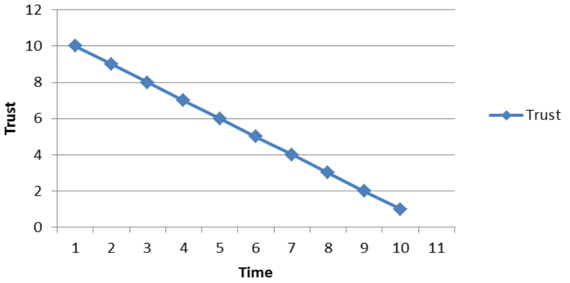

Figure 8 Trust of a black hole node with respective time.

c. Energy consumption of nodes:

Assume that the energy threshold is Θ=10. When the black hole is generated it is consumed more energy than the threshold. Fig.7 shows some nodes are consumed more energy than the threshold, so easily those nodes are deducted from path.

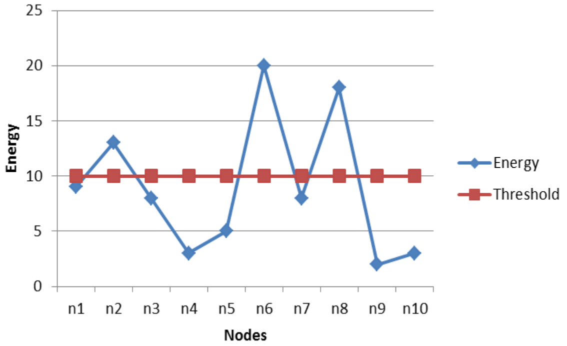

Figure 9 Energy consumption at different nodes.

VII. CONCLUSION

In this paper, we have proposed Trust Based Secure Routing. The scheme based on secure routing detection, to achieve high successful routing probability, security and scalability. The scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve successful routing Probability. High energy efficiency is also achieved by avoiding the black holes. The theoretical analysis and experimental results have shown that the scheme improves the successful routing. Further, the scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor network security.

VIII. REFERENCES

[1] 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.

[2] 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.

[3] M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEETransactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

[4] 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.

[5] 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.

[6] H. Sun, C. Chen, Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, pp. 1-4, 2007.

[7] 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.

[8] W. Lou, Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Transaction on vehicular technology, vol. 55, no. 4, pp. 1320-1330, 2006.

[9] Y. Liu, Y. Zhu, L. M. Ni, et al. "A reliability-oriented transmission service in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 12, pp. 2100-2107, 2011.

[10] G. X. Zhan, W. S. Shi, J. L. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, 2012.

[11] 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.