# Energy Efficient Secure and Trustable Routing In Wireless Sensor Networks

**E. Vinothini[1], Dr. G. Ramachandran[2]**
[1, 2] Department of Computer Science and Engineering
[1, 2] Annamalai University, Chidambaram, India

***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 ActiveTrust is proposed for WSNs. The most important innovation of ActiveTrust 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 improves the data route security. More importantly, the generation and distribution of detection routes are given in the ActiveTrust scheme, which can fully use the energy in non-hotspots to create as many detection routes as needed to achieve the desired security and energy efficiency. ActiveTrust can significantly improve the data route success probability and ability against black hole attacks and can optimize network lifetime. A method is contributed to energy efficient alternate path selection for future data transmission.*

***Keywords***- Black hole attack, network lifetime, security, trust, wireless sensor networks.

## I. INTRODUCTION

Of the various possible security threats that may be experienced by a wireless sensor network (WSN), in this thesis specifically interested in combating two types of attacks: the compromised-node (CN) attack and the denial-of-service (DOS) attack [13]. The CN attack refers to the situation when an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the WSN by actively disrupting, changing, or even destroying the functionality of a subset of nodes in the system. These two attacks are similar in the sense that they both generate black holes: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes [5]. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it [1]. At the same time, an adversary can always perform certain form of DOS attack (e.g., jamming) even if it does not have any knowledge of the crypto-system used in the WSN. 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 [14]. A 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, 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

- To improve the data route security.
- To improve the energy efficiency and network lifetime.
- To improve the detection accuracy

Hence, the main contribution of this article is to energy efficient alternate path selection for future data transmission. The rest of the paper organized as follows. Section II gives an overview of related works. Section III System architecture of ActiveTrust Scheme. Section IV modules of my paper. Section V Results and discussion. Our proposed protocol can achieve better security performance. First, nodes with high trust is chosen to avoid potential attack, and then the route is chosen along a successful detection route. Through the above approach, the network security can be improved.

## II. WIRELESS SENSOR NETWORKS

A Wireless Sensor Network(WSN) is a distributed network and it comprises a large number of distributed, self-

directed, tiny, low powered device called nodes alias motes. WSN naturally encompasses a large number of spatially dispersed, petite, battery-operated, embedded device that are networked to supportively collect, process and convey data to the users, and it has restricted computing and processing capabilities. Motes are the small computers, which work collectively to form the networks. Motes are energy efficient, multi-functional wireless device. The necessities for motes in industrial applications are widespread. A group of motes collect the information from the environment to accomplish particular application objectives. They make links with each other in different configurations to get the maximum performance. Motes communicate with each other using transceiver. In WSN the number of sensor nodes can be in the order of hundreds or even thousands.

Nowadays wireless network is the most popular services utilized in industrial and commercial applications, because of its technical advancement in processor, communication, and usage of low power embedded computing devices. Sensor nodes are used to monitor environmental conditions like temperature, pressure, humidity, sound, vibration, position etc. In many real time applications the sensor nodes are performing different tasks like neighbor node discovery, smart sensing, data storage and processing, data aggregation, target tracking control and monitoring node localization synchronization and efficient routing between nodes and base stations.

## III. RELATED WORKS

In this section the paper are related to the aspects of security maintenance in WSN using Active Trust Scheme.

T. P. Nghiem, T. H. Cho have described a multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks [10]. A compromised node can generate a fabricated report, which results in false alarms, information loss, and a waste of precious network energy. An interleaved hop-by-hop authentication (IHA) scheme has been proposed to minimize such serious damage by detecting and filtering false reports at the very early en-route nodes. Unfortunately, IHA, with a single path from the source to the BS, cannot keep its security goal if more than t intermediate nodes are compromised. In this paper, an enhanced multi-path interleaved hop-by-hop authentication (MIHA) scheme is proposed. MIHA sets up disjoint and braided paths and switches to alternate paths when there is more than t compromised nodes on the current path to continue dealing with en-route insider attacks. A new key assignment mechanism was also applied to enhance network security and to reduce key storage overhead.

Y. Hu, A. Liu have described An Efficient Heuristic Subtraction Deployment Strategy to Guarantee Quality of Event Detection for WSN's. Cooperative sensing and monitoring event is one of the important applications of sensor networks [2]. Node deployment and duty cycle configuration of event detection in a large wireless sensor networks is an enormous challenge. In this paper, through in-depth analysis we find that there is a tradeoff between node duty cycle and event quality monitoring. That is, adopting larger duty cycle enables network to deploy fewer nodes. Or deploying more nodes can reduce their duty cycle. Both of them can reach the event detecting quality requirement of application. Based on the above findings, a novel subtraction deployment strategy (SDS) combined with the unequal node duty cycle in the network is presented. This strategy improves the duty cycle of nodes in non-hotspots area when reduces the number, thereby minimizing the deployment cost on the premise of meeting the detecting quality of application. Introduce a formal model to indicate the tradeoff between deployment cost and the quality of event detection.

J. Wang, Y. H. Liu, Y. Jiao: Building a trusted route in a mobile ad hoc network considering communication reliability and path length. In a mobile ad hoc network (MANET), [8] a source node must rely on other nodes to forward its packets on multi-hop routes to the destination. Unlike most previous studies that sought only the shortest path, our study proposes a novel trusted route that considers communication reliability and path length for a reliable and feasible packet delivery in a MANET. In most MANET routing schemes, security is an added layer above the routing layer. We introduce the concept of attribute similarity in finding potentially friendly nodes among strangers; so security is inherently integrated into the routing protocol where nodes evaluate trust levels of others based on a set of attributes. Unlike the fixed probability of dropping packets adopted in other routing mechanisms, our new forwarding rule is designed based on the attribute similarity and provides a recommended method in calculating the degree of similarity between attributes.

I. Aad, P. J. Hubaux and W. E. Knightly have described the Impact of Denial of Service Attacks on Ad Hoc Networks. Significant progress has been made towards making ad hoc networks secure and DoS resilient. However, little attention has been focused on quantifying DoS resilience: Do ad hoc networks have sufficiently redundant paths and counter-DoS mechanisms to make DoS attacks largely ineffective? Or are there attack and system factors that can lead to devastating effects? In this paper, design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause [13]. The first attack called the

JellyFish attack, is targeted against closed-loop flows such as TCP; although protocol compliant, it has devastating effects. The second is the Black Hole attack, which has effects similar to the Jellyfish, but on open-loop flows. Quantify via simulations and analytical modeling the scalability of DoS attacks as a function of key performance parameters such as mobility, system size, node density, and counter-DoS strategy.

T. Shu, M. Krunz, S. Liu have described the Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs) [11]. In this paper, study routing mechanisms that circumvent (bypass) black holes formed by these attacks. That existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, develop mechanisms that generate randomized multi-path routes. Under our design, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost.

G. X. Zhan, W. S. Shi, J. L. Deng J L have described SensorTrust: A resilient trust model for wireless sensing systems. Wireless sensor networks (WSNs) are prone to failures and malicious attacks. Traditional approaches from encryption and authentication are not sufficient to solve the problems [5]. Trust management of WSNs is bringing new approaches. However, it is still a challenge to establish a trust environment for WSNs. To conquer that challenge, propose a resilient trust model with a focus on data integrity, SensorTrust, for hierarchical WSNs. SensorTrust integrates past history and recent risk to accurately identify the current trust level. It employs a Gaussian model to rate data integrity in a fine-grained style and a flexible update protocol to adapt to varied context. With acceptable overhead, SensorTrust proves resilient against varied faults and attacks.

F. Gómez Mármol, G. Martínez Pérez have described the TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks Vehicular ad hoc networks (VANETs) have drawn the attention of a number of researchers due to their several advantages and benefits [6]. It is a very promising area of knowledge where investing new funds and effort is surely a wise move. Nevertheless, despite their multiple capabilities, new unresolved risks arise, and it is not always easy, or even feasible to cope with them. Recently, trust and reputation management has been proposed as a novel and accurate way to deal with some of these deficiencies. A considerable amount of works have been developed so far in this field concerning P2P networks, wireless sensor networks, ad hoc networks, etc. However, the application of behavioral-based trust and reputation management to VANETs is still at a preliminary stage. In this paper survey the state of the art, proving the current lack of proposals in this specific environment. We also suggest a set of design requirements for trust and reputation models specifically applicable to VANETs. Furthermore, the original proposal, TRIP, aimed to quickly and accurately distinguish malicious or selfish nodes spreading false or bogus messages throughout the network. The level of fulfillment of each of the surveyed models with regard to each design requirement suggestion, comparing them with this approach.

## IV. SYSTEM OVERVIEW

### ACTIVE TRUST SCHEME

In this section discuss about an overview of Active Trust scheme, which is composed of an active detection routing protocol and Data routing protocol (Fig.1).

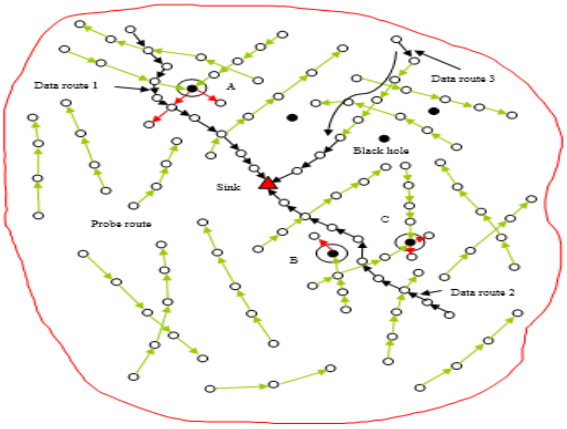


Figure 1. Active Trust Scheme

Fig.1 shows that architecture of active trust scheme is proposed to implement the, the source node randomly selects an undetected neighbor node to create an active detection route. 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.

## V. MODULES

### A. Black Hole Attack

A 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, resulting in sensitive data being discarded or unable to be forwarded to the sink [10]. 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 [7].

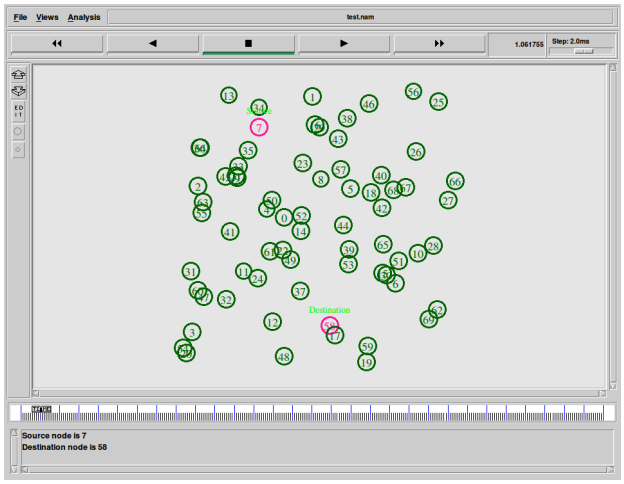


Figure 2. Network Environment

The architecture of network with random number of nodes green in color. The node 7 which is pink in color represents the source node from where the packets are transmitted to the destination node 58 through the intermediate nodes

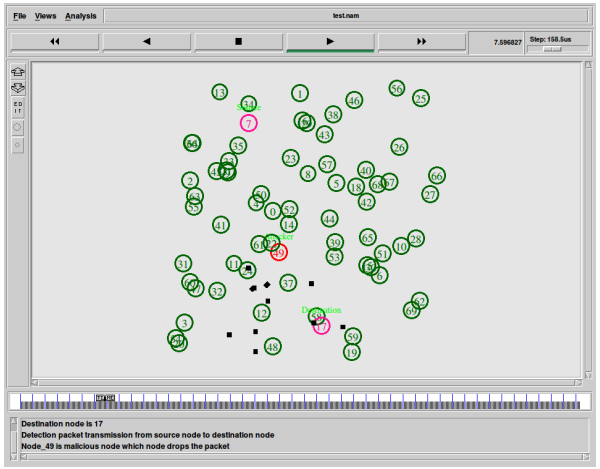


Figure 3. Black Hole Attack

The Black hole attacker node is indicated by red color. It drops the packets forwarded through it as shown in Fig.3

## B. 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 [11]. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes [5]. 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 [15]. In this scheme, the source node randomly selects an undetected neighbor node to create an active detection route [10]. Considering that the longest detection route length [8], the detection route decreases its length by 1 for every hop until the length is decreased to 0, and then the detection route ends [14].

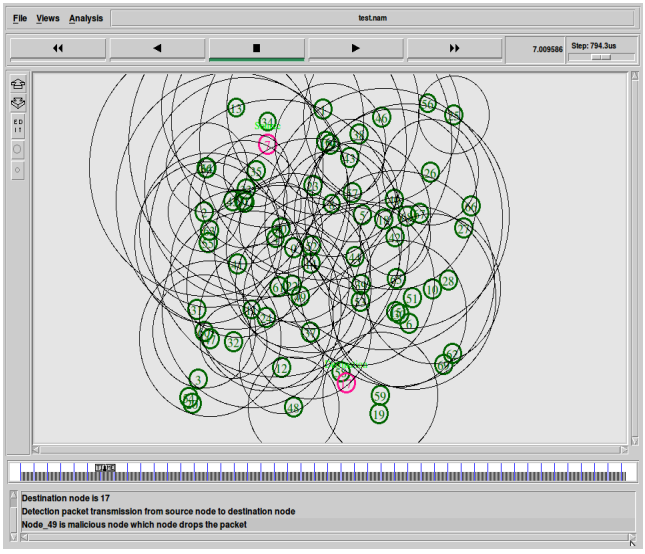


Figure 4. Data Transmission

The Data transmission between source and destination. The path is identified through 7-49-17 as shown in Fig.4.

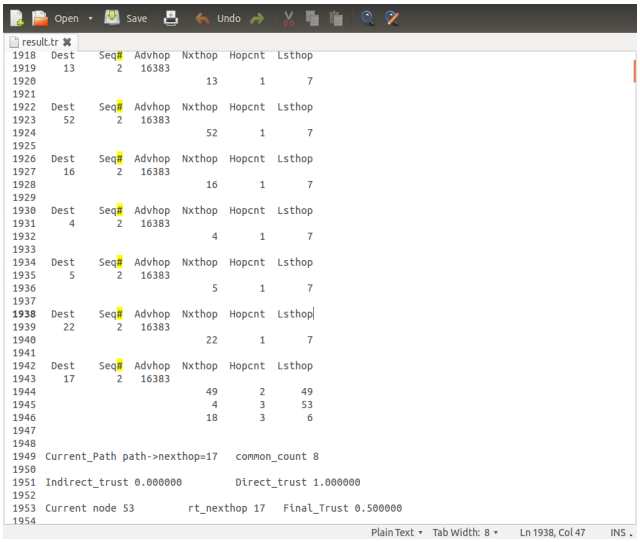


Figure 5. Active Detection Routing Protocol

Multiple routes are found between Source and destination as shown in Fig.5.

**Routing overhead**

Wireless sensor networks are designed to be scalable.as the network grows, various routing protocols perform differently. The amount of routing traffic increases as the network grows [8]. An important measures of the scalability of the protocol, and thus the network, is its routing overhead. It is defined as the total number of routing packets transmitted over the network, expressed in bits per second or packets per second.

### C. Data Routing Protocol

The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs. The difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink [8]. The attacker is found in data routing based on threshold value. If router final trust value is greater than threshold means it is selected as next hop otherwise it is attacker [15]. The 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; [11] similarly, if it cannot find any such appropriate next hop, it sends a feedback failure to its upper node.

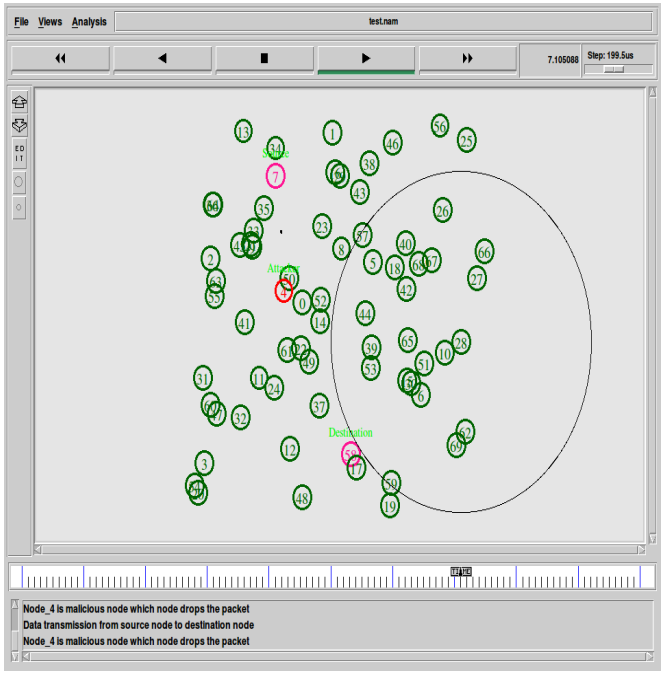


Figure 6. Detection Packet Transmission

Fig.6 shows that the data transmission between source to destination. The path is 7-4-58 and black hole attacker is 4.

The router having highest trust value it selected as next hop of corresponding source. So, the destination received the data from highest trust value routers. Detection packet is sent from source to destination through three available routes [14]. The feedback packet is accepted by source that is sent by destination in first route. When black hole attack is launched in a route the attacker drops all the detection packet. So the feedback packet is not delivered to source that is sent by destination.

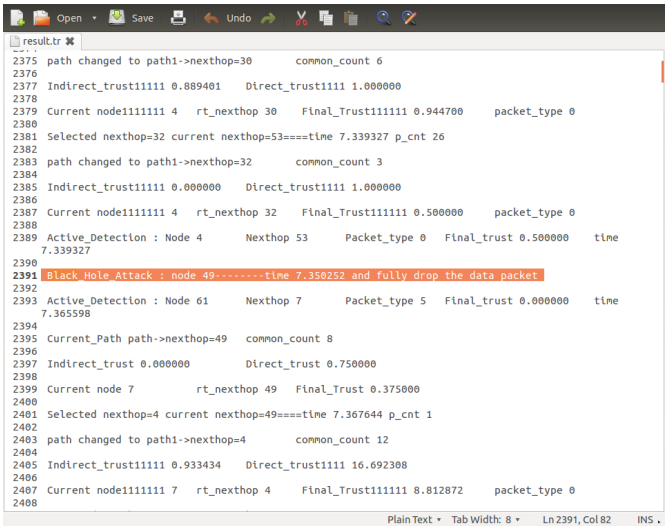


Figure 7. Feedback Packets

Fig.7 shows the feedback packet is not delivered to source that is sent by destination first route (7-49-17)

**Trust Maintenance**

Two trust value is maintained for each node based on forward count, received count and drop count [7].

Direct Trust value (Trust1) = forward count of packet / received count of packet
Trust2 = drop count of packet / received count of packet
If Trust1 value is increased the detection packet is successfully delivered.
If Trust2 value is decreased the detection packet is dropped.

**Indirect Trust Maintenance**

The calculation of indirect trust value based on common neighbours reported trust value of corresponding node, common neighbour count [7]. The Total trust value is calculated based on average value of direct trust and indirect trust value of corresponding next hop.

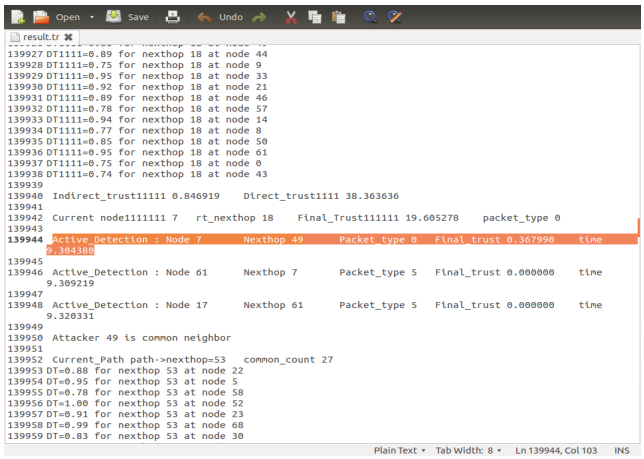


Figure 8. Trust Value Calculation

The total trust value is reduced for attacker in detection packet transmission as shown in fig.8

**D. Energy Efficient Alternate Path Selection**

After Black hole attack identification intrusion response mechanism is required to prevent the network performance degradation due to attacker. In intrusion response mechanism, [3] the attacker is classified as black hole attacker, and alternate path with high trust and energy efficiency that excludes attacker is found for future data transmission.

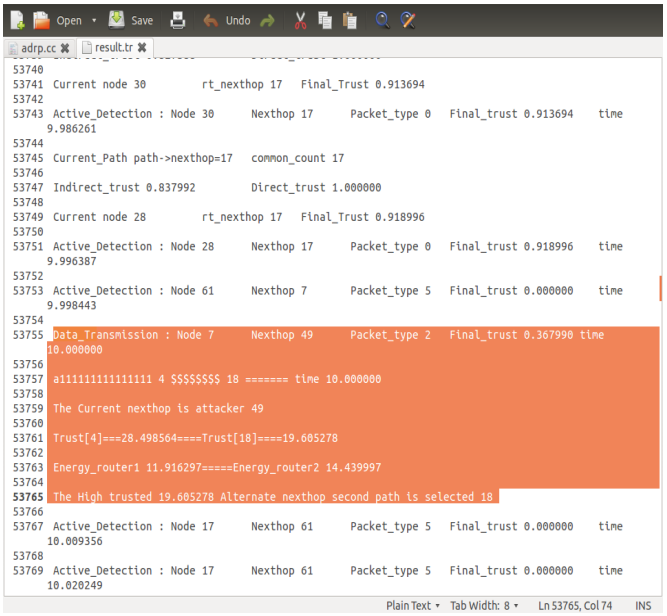


Figure 9. Next Hop Selection

The next hop is selected based on energy in enhanced technique as shown in fig.9

## VI. RESULTS AND DISCUSSION.

The performance of Active Trust scheme is analyzed using network simulator2. The experimental mode l is built with 70 nodes distributed randomly on square of 600 × 600 .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 proposed approach creates multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes,[10] it will attack these routes and, while doing so, the attacker is 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 [15]. 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 [4]. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes. However, it possible after carefully analyzing the energy consumption in WSNs. There is still up to 90% residual energy in WSNs when the network has died due to the "energy hole" phenomenon. Therefore, the ActiveTrust scheme takes full advantage of the residual energy to create detection routes and attempts to decrease energy consumption in hotspots (to improve network lifetime) [7]. Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security. The Active Trust scheme has better security performance. First, nodes with high trust is chosen to avoid potential attack, and then the route is

chosen along a successful detection route. Through the above approach, the network security can be improved.

## VII. PERFORMANCES AND EVALUATION

### a. Simulation Model

| | |
|---|---|
| SIMULATOR | Network Simulator 2 |
| TOPOLOGY | Random |
| INTERFACE TYPE | Phy /WirelessPhy |
| MAC TYPE | IEEE 802.11 |
| QUEUE TYPE | Drop Tail/Priority Queue |
| QUEUE LENGTH | 50 Packets |
| ANTENNA TYPE | Omni Antenna |
| PROPAGATION TYPE | Two Ray Ground |
| ROUTING PROTOCOL | AOMDV |
| TRANSPORT AGENT | UDP |
| APPLICATION AGENT | CBR |
| NERWORK AREA | 500 * 500 |
| NUMBER OF NODES | 70 |
| SIMULATION TIME | 100seconds |

## VIII. PERFORMANCE EVALUATION

### Energy Consumption

Energy consumption is defined as the amount of energy consumed for the network operation and data transmission.

### Detection Accuracy

The detection accuracy is defined as the number of intrusion instances detected by the system divided by the total number of intrusion instances present in the network.

### Throughput

It is the amount of data successfully reached at the destination.
Throughput (bits / s) = Total Data / Data Transmission Duration

### Comparative Graph

### Throughput

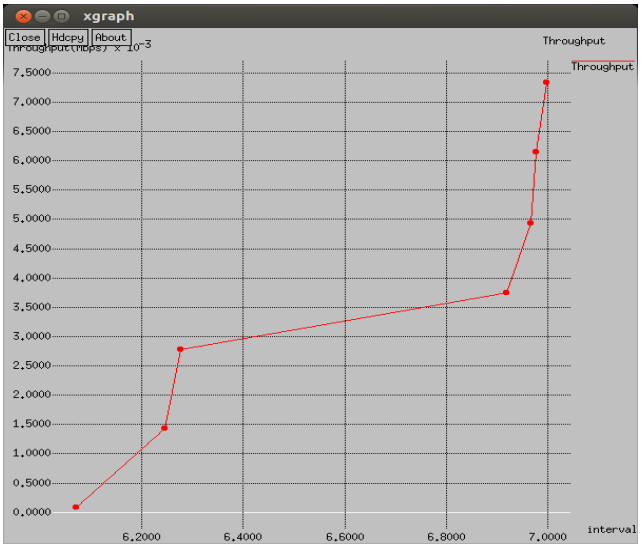


Figure 10. shows that x-axis represent the number of nodes and y-axis represents the throughput (Mbps) which is the measurement of the number of packets passing through the network over a unit of time. Through increases when compared to the existing work.

### Energy Consumption

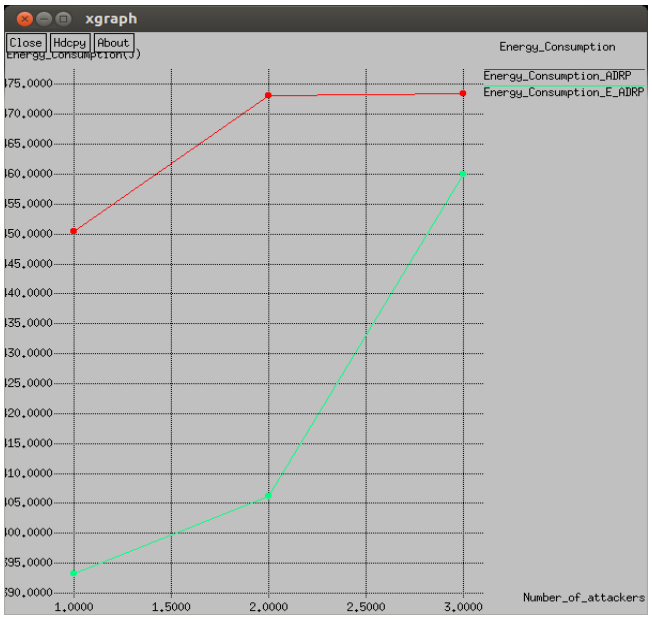


Figure 11. shows that the X axis represents Number of Attackers and the Y axis represents Energy Consumption (Joules). Here E_ADRP achieves reduced energy consumption when compared to ADRP method.

### Actual Residual Energy

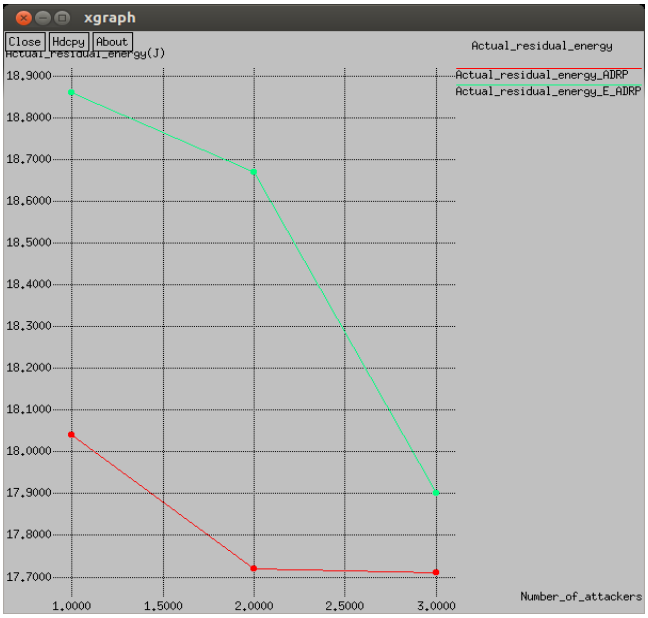


Figure 12. shows that the X axis represents Number of Attackers and the Y axis represents Actual Residual Energy (Joules).E_ADRP maintains increased actual residual energy in the network when compared to ADRP method.

**Dead Node Count**

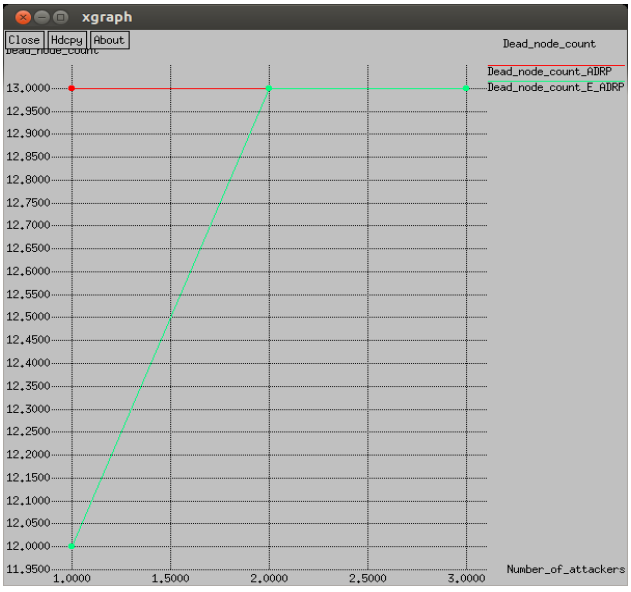


Figure 13. shows that the X axis represents the Number of Attackers and the Y axis represents the Dead Node Count. E_ADRP achieves reduced dead node count when compared to ADRP method.

## IX. CONCLUSION

In proposed system 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 a nearly 100% successful routing probability. (2) High energy efficiency. The Active Trust scheme fully uses residue energy to construct multiple detection routes. A method is contributed to energy efficient alternate path selection for future data transmission.

## REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] G. X. Zhan, W. S. Shi, J. L. Deng J L, "SensorTrust: A resilient trust model for wireless sensing systems," Pervasive and Mobile Computing, vol. 7, no. 4, pp. 509-522, 2012.

[6] F. Gómez Mármol, G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934-941.2012.

[7] 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.

[8] J. Wang, Y. H. Liu, Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1138-1149, 2011.

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

[10] 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.

[11] 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.

[12] Teerawat Iassariyakul, Ekram Hossain, "Introduction to Network Simulator NS2" Springer,2009.

[13] I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, vol. 16, no. 4, pp. 791- 802, 2008.

[14] 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.

[15] M. Y. Hsieh, Y. M. Huang, H. C. Chao, "Adaptive security design with malicious node detection in cluster-based sensor networks," Computer Communications, vol. 30, no. 1, pp. 2385-2400, 2007.