A Secure and Efficient Routing protocol in Multi-hop Wireless Networks

[1] Gembali Sateesh, [2] Dr S. Jhansi Rani

[1]M.Tech Scholar, Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.

[2]Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.

***Abstract*:** In the existing system, the nodes break the route due to malicious attacks. The Packet delivery latency is increased due to the breaking of routes. In the proposed system, the routing path is selected based on the request response method. The source node checks the hashing neighbor nodes id, data with timestamp. Then it transmits the data to destination using e-star protocol. Each and every node while registering, server provides them with id, primary key, secondary key and decryption key. Source collects the primary key of all the intermediate nodes. It also finds the optimum path. We encrypt the data using the AES algorithm. The wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. The id and secondary key is collected and it is transmitted to both the source and the destination. Similarly all the id's and secondary key are collected and concatenated, so as to verify both source and destination. Tpa implementation is also achieved for successful validation of concatenated keys and reward is provided to the intermediate hops. Problem Definition: In this paper we improve the security and reduce the packet delay and prevent data in adversary environment**.**

***Keywords*: Multihop packet transmission CPU AES algorithm and PDA.**

1. INTRODUCTION

In a Wireless Sensor Networks a mobile node communicates with a remote destination. It relies on the other nodes to relay the packets. Network Coverage can be extended in Multihop packet transmission by using limited power and improved area spectral efficiency. In developing and rural areas, the network can be deployed more readily and at low cost. In civilian applications of multi hop wireless networks, the nodes have long relation with the network. In heterogeneous multi hop wireless networks (HMWNs), the nodes' mobility level and hardware/energy resources varies. HMWNs implements many useful applications such as data sharing and multimedia data transmission. For example, users in one area (residential neighborhood, university campus, etc) has different wireless-enabled devices (PDAs, laptops, tablets, cell phones, etc.) can establish a network to communicate, distribute files, and share information. In military and disaster-recovery applications, the nodes' behavior is highly predictable because the network is closed and the nodes are controlled by one authority. However, the nodes' behavior is unpredictable in civilian applications for different reasons. The nodes are typically autonomous and self-interested and may belong to different authorities. The nodes also have different hardware and energy capabilities and may pursue different goals. In addition, malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software, and malicious nodes actively break routes to disrupt data transmission. Since the mobile nodes are battery driven and one of the major sources of energy consumption is radio transmission, selfish nodes are unwilling to lose their battery energy in relaying other users' packets. When more nodes are cooperative in relaying packets, the routes are shorter, the network connectivity is more, and the possibility of network partition is lower. Moreover, since the nodes are equipped with different hardware capability, such as CPU speed and buffer size, the nodes having large hardware resources can perform packet relay more successfully than others.

2 SIMULATION ENVIRONMENTS

ns is a discrete event simulator developed by the University of California at Berkeley and the VINT project [6]. While it provides substantial support for simulating TCP and other protocols over conventional networks, it provides no support for accurately simulating the physical aspects of multi-hop wireless networks or the MAC protocols needed in such environments. Berkeley has recently released ns code that provides some support for modeling wireless LANs, but this code cannot be used for studying multi-hop ad hoc networks as it does not support the notion of node position; there is no spatial diversity (all nodes are in the same collision domain), and it can only model directly connected nodes. In this section, we describe some of the modifications we made to ns to allow accurate simulation of mobile wireless networks.

2.1 PHYSICAL AND DATA LINK LAYER MODEL

To accurately model the attenuation of radio waves between antennas close to the ground, radio engineers typically use a model that attenuates the power of a signal as 1————————————2 at short distances (is the distance between the antennas), and as 1————————————4 at longer distances. The crossover point is called the reference distance, and is typically around 100 meters for outdoor low-gain antennas 1.5m above the ground plane operating in the 1–2GHz band [20]. Following this practice, our signal propagation model combines both a free space propagation model and a two-ray ground reflection model. When a transmitter is within the reference distance of the receiver, we use the free space model where the signal attenuates as 1————————————2. Outside of this distance, we use the ground reflection model where the signal falls off as 1 4. Each mobile node has a position and a velocity and moves around on a topography that is specified using either a digital elevation map or a flat grid. The position of a mobile node can be calculated as a function of time, and is used by the radio propagation model to calculate the propagation delay from one node to another and to determine the power level of a received signal at each mobile node. Each mobile node has one or more wireless network interfaces, with all interfaces of the same type (on all mobile nodes) linked together by a single physical channel. When a network interface transmits a packet, it passes the packet to the appropriate physical channel object. This object then computes the propagation delay from the sender to every other interface on the channel and schedules a "packet reception" event for each. This event notifies the receiving interface that the first bit of a new packet has arrived. At this time, the power level at which the packet was received is compared to two different values: the carrier sense threshold and the receive threshold. If the power level falls below the carrier sense threshold, the packet is discarded as noise. If the received power level is above the carrier sense threshold but below the receive threshold, the packet is marked as a packet in error before being passed to the MAC layer. Otherwise, the packet is simply handed up to the MAC layer. Once the MAC layer receives a packet, it checks to insure that its receive state is presently "idle." If the receiver is not idle, one of two things can happen. If the power level of the packet already being received is at least 10 dB greater than the received power level of the new packet, we assume capture, discard the new packet, and allow the receiving interface to continue with its current receive operation. Otherwise, a collision occurs and both packets are dropped. If the MAC layer is idle when an incoming packet is passed up from the network interface, it simply computes the transmission time of the packet and schedules a "packet reception complete" event for itself. When this event occurs, the MAC layer verifies that the packet is error-free, performs destination address filtering, and passes the packet up the protocol stack.

2.2 MEDIUM ACCESS CONTROL

The link layer of our simulator implements the complete IEEE 802.11 standard [8] Medium Access Control (MAC) protocol Distributed Coordination Function (DCF) in order to accurately model the contention of nodes for the wireless medium. DCF is similar to MACA [11] and MACAW [1] and is designed to use both physical carrier sense and virtual carrier sense mechanisms to reduce the probability of collisions due to hidden terminals. The transmission of each unicast packet is preceded by a Request-to-Send/Clear-to-Send (RTS/CTS) exchange that reserves the wireless channel for transmission of a data packet. Each correctly received unicast packet is followed by an Acknowledgment (ACK) to the sender, which retransmits the packet a limited number of times until this ACK is received. Broadcast packets are sent only when virtual and physical carrier
sense indicate that the medium is clear, but they are not preceded by an RTS/CTS and are not acknowledged by their recipients.

2.3 ADDRESS RESOLUTION

Since the routing protocols all operate at the network layer using IP addresses, an implementation of ARP [19], modeled after the BSD Unix implementation [23], was included in the simulation and used to resolve IP addresses to link layer addresses. The broadcast nature of an ARP REQUEST packet (Section 6.3) and the interaction of ARP with on-demand protocols (Section 6.4) make ARP an important detail of the simulation.

2.4 PACKET BUFFERING

Each node has a queue for packets awaiting transmission by the network interface that holds up to 50 packets and is managed in a drop-tail fashion. Each on-demand routing protocol (i.e., TORA, DSR, or AODV), can buffer separately an additional 50 packets that that are awaiting discovery of a route through the network.

3. LITERATURE REVIEW

Performance Evaluation of on demand routing Protocols Aodv and Modified Aodv (R-Aodv) In Manets: In mobile ad hoc networks, there is no centralized infrastructure to monitor or allocate the resources used by the mobile nodes. The absence of any central coordinator makes the routing a complex one compared to cellular networks. The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile devices. AODV uses an on demand approach for finding routes. AODV and most of the on demand ad hoc routing protocols use single route reply along the reverse path. Due to rapid changes of topology the route reply may not arrive to the source node resulting in sending several route request messages and degrading the performance of the routing protocol. The extended AODV called Reverse Ad Hoc on Demand Vector (R-AODV) protocol uses a reverse route discovery mechanism and performs well when link breakage is frequent. In this paper we compare the QoS parameters such as Throughput, Delay and Packet Delivery ratio of both traditional AODV and R-AODV using TCP New Reno as the traffic source. Simulation results show that R-AODV performs well when link breakage is frequent.

An Anonymous On Demand Routing Protocol With Untraceable Routes For Mobile Ad-Hoc Networks: In hostile environments, the enemy can launch traffic analysis against intercept able routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For route anonymity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on “broadcast with trapdoor information”, a novel network security concept which includes features of two existing network and security mechanisms, namely “broadcast” and “trapdoor information”. We use simulations and implementation to validate the effectiveness of our design.

An Efficient Secure Distributed Anonymous Routing Protocol For Mobile And Wireless Ad Hoc Networks: An ad hoc wireless network is a temporary and dynamic environment where a group of mobile nodes with radio frequency transceivers communicate with each other without the intervention of any centralized administration or established infrastructure. Due to the limited transmission range of each mobile node, communication sessions between two nodes are usually established through a number of intermediate nodes, which are supposed to be willing to cooperate while forwarding the messages they receive to their destination. Unfortunately, some of these intermediate nodes might not be trustworthy and might be malicious, thereby forming a threat to the security and/or confidentiality of the exchanged data between the mobile nodes. While data encryption can protect the content exchanged between nodes, analysis of communication patterns may reveal valuable information about end users and their relationships. Using anonymous paths for communication provides security and privacy against traffic analysis. To establish these anonymous paths, in a traditional wired network, nodes build a global view of the network by exchanging routing information, whereas in an ad hoc wireless network, building this global view is not an option. In this paper, we propose a novel distributed routing protocol which guarantees security, anonymity and high reliability of the established route in a hostile

environment, such as ad hoc wireless network, by encrypting routing packet header and abstaining from using unreliable intermediate node. The major objective of our protocol is to allow trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes. We describe our protocol, and provide its proof of correctness.

Secure Neighbor Discovery System for Ad-Hoc through Aasr Protocol: Unknown accessing is important for many applications in MANET in adversary environments. The main aim of network is to provide unidentifiability and unlink ability for mobile nodes. In this proposed system a new routing protocol, i.e., authenticated anonymous secure routing (AASR), to satisfy the requirement and defend the attacks has been used. More specifically, the route request packets are authenticated by a group signature, to defend the potential active attacks

without unveiling the node identities. By improving AASR, the packet delay can be reduced. A possible method is to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks. By gathering the link quality of each and every node within the path between sources to destination in network will be helpful for increasing the energy of the network and to achieve the energy efficient network.

4. System Analysis

In the existing system, malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency.

A. Demerits

Waiting time is increased, unreliable, less data transmission rate, less effective in the proposed system, based on request response source selects routing path. After that source hashing neighbor nodes id, data with timestamp. Then it transmits the data to destination using e-star protocol. In the modification process, the modification is our implementation. Where we deploy onion protocol. Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Source will find out the optimum path and it will collect primary key of all intermediate node. Data's first encrypted using AES algorithm and then with corresponding primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Then collecting its id and secondary key which is transmitted to both source and destination node. Same way all the id's and secondary key are collected and concatenated, so as to verify both source and destination. TPA implementation is also achieved for successful validation.

B. Advantages

Waiting time is decreased, reliable, high data transmission rate more effective, high security

C. Implementation: Network Construction

In this Paper, first we have to construct a network which consists of 'n' number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, we can assume that the nodes are moving across the network. Network is used to store all the Nodes information like Node Id and other information. Each node is having primary key, secondary key and private key. Also network will monitor all the Nodes Communication for security purpose.

D. Route request based on routing table checking

In this module, source node sends hello interval request to all intermediate nodes for identifying minimum hop count, capacity of intermediate nodes, based on node connectivity. It can use the routing table in the RREQ packet to estimate how many its neighbors have not been covered by the RREQ packet from previous intermediate node. Each intermediate node validates the RREQ packet and updates its routing tables. Finally RREQ reaches to destination node.

E. Route selection and source side encryption process

In this module, the RREQ is received and verified by the destination node. The destination node selects the route based on hop count and throughput. Then the destination node assembles an RREP packet and broadcasts it back to the source node. Each intermediate node validates the RRES packet and updates its routing tables. After route selection, source encrypts the data based on AES encryption and it collects the selected neighbor nodes public key from routing table. Although source conducts the encryption process based on selected route public keys using AASR protocol based on onion routing.

F. Packet Forwarding

In this module, source node forwards the encrypted packet to neighbor node based on selected route. Neighbor node gives its own private key for one part of decryption process. After that it will send to next neighbor node. Similarly each neighbor nodes in selected route decrypts the packet based on its private key using AASR protocol. Sometime attacker node also receives the packets.

G. Decryption Process

In this module, neighbor node decrypts the packet and finally sends to destination node. Then the destination node decrypts the packet with its private key and AES decryption key. Finally destination node views the original data. Since the paths capacity will vary dynamically, so that the paths will be changed dynamically as per data transfer along the network. So it increases the packet delivery ratio and decreases the average end-to-end delay.

H. TPA verification and payment process

In this module, after data transmission each intermediate node in selected path sends its id and secondary key to trusted party auditor. Destination node also sends the id and secondary keys of selected nodes to TPA after data retrieval from source node. Then TPA audits the both id and secondary keys are match or not based on ESTAR protocol. If match means TPA rewards to that trusted node. Suppose it mismatch it easily identify the attacker node.

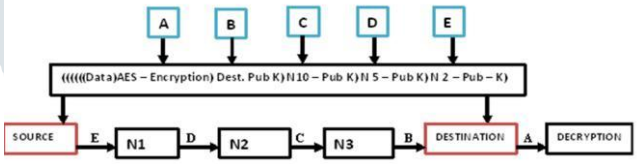
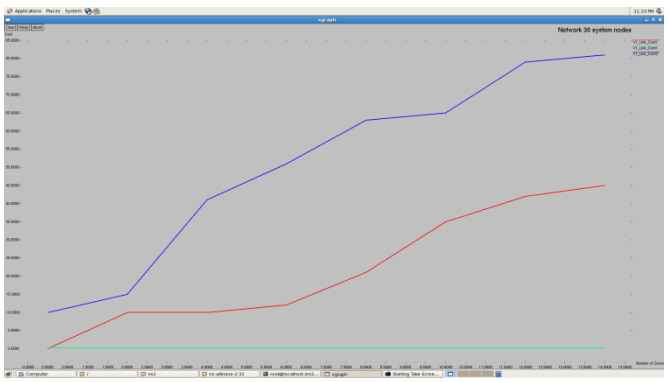
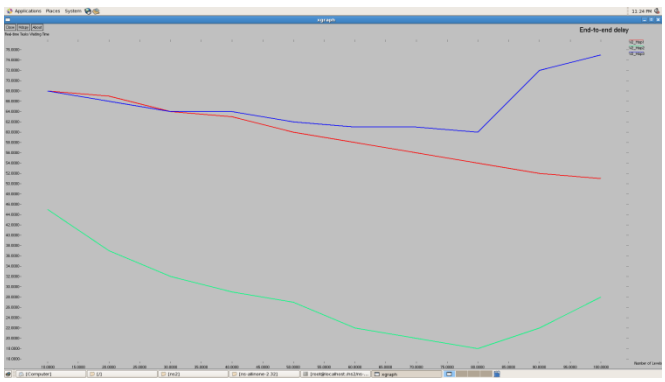


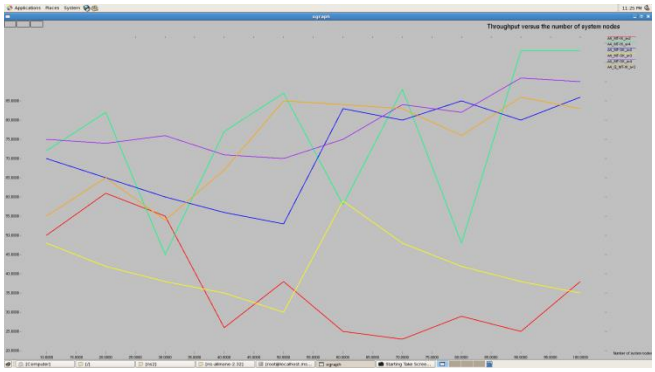
Fig. 1. Architecture diagram

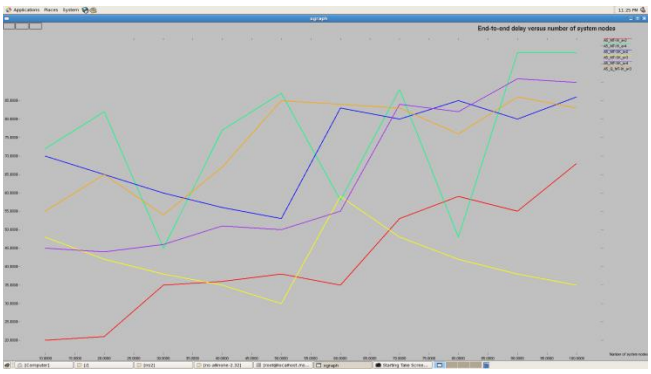
5. TESTING STRATEGIES

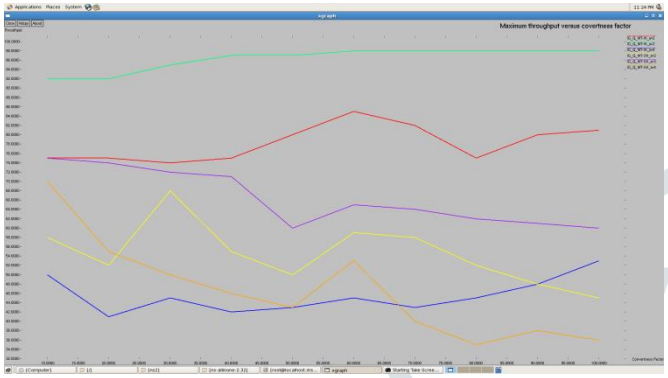
A number of software testing strategies have been proposed in the literature. All provide the software developer with a template for testing and all have the following generic characteristics: Testing begins at the component level and works “outward” toward the integration of the entire computer-based system. Different testing techniques are appropriate at different points in time. The developer of the software conducts testing and for large projects, independent test group. Testing and debugging are different activate accommodated in any testing strategy.

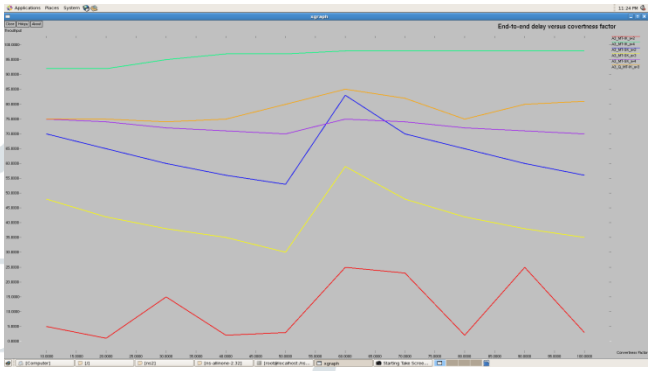












6. Conclusion

We have proposed E-STAR that uses payment/trust systems with trust-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. E-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. We have proposed SRR and BAR routing protocols and evaluated them in terms of overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behavior, and the route lifetime based on the nodes' energy capability. SRR establishes routes that can meet source nodes' trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR. The analytical results have demonstrated that E-STAR can secure the payment and trust calculation without false accusations. Moreover, the simulation results have demonstrated that E-STAR can improve the packet delivery ratio due to establishing stable routes.

7. Future Enhancements

To ensure Data security and privacy data is spitted into multiple block encrypted and stored in multiple images to ensure security

REFERENCES

G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.

X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242, 2012.

G. Indirania and K. Selvakumara, "A Swarm-Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014

H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.

K. Liu, J. Deng, and K. Balakrishnan, "An Acknowledgement- Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007

S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.