International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.6., 2015
(Nov.-Dec.,)

RESEARCH ARTICLE

ISSN: 2321-7758

ANONYMOUS ENCRYPTION SECURE ROUTING IN MOBILE AD HOC NETWORKS

S.SRITHAR[1], Dr.K.KARUPPASAMY[2]

[1]Assistant Professor, [2]Professor & Head

Department of Information Technology, RVS College of Engineering and Technology,
Coimbatore, Tamil Nadu, India

S.SRITHAR

Dr.K.KARUPPASAMY

ABSTRACT

Efficient defense against security attacks is a challenging task in the Mobile Ad Hoc Networks and offering security guarantees and developing an network protocols for that. Geographical routing which greatly avoids routing attacks, which focus on multi dimensional trust management features. A significant research issues is to design of trust model to detect the malicious accesses from direct and indirect attacks. Once trust information is available for all network nodes, the routing decisions can take it into account, i.e. routing can be based on both location and trust attributes (hidden servers). The situation is further aggravated as the next generation MANET will be larger and larger. To face this problem, we propose a Anonymous Encryption secure routing protocol (AESER) which adopts the geographical routing principle to cope with the network dimensions and relies on a distributed trust model (hidden servers) for the avoidance of malicious nodes.

Keywords-MANET, AESER.

I. INTRODUCTION

Mobile Adhoc Network is self organized networks. A mobile adhoc network is collection of mobile nodes that communicate to other mobile nodes. Due to nature of mobile nodes it can move in any direction. The main problem of mobile nodes is topology changes. In this routing between the nodes is complicated due to security. So we need to provide security mechanism for the mobile nodes. In our proposed approach shows how a security issues is solved in node to node communication.

II. LITERATURE SURVEY

Stefaan Seys and Bart Preneel [1] Proposed and investigates anonymity of the network nodes. Anonymity is an important part of the overall security Architecture for mobile ad hoc networks as it allows users to hide their activities. This enables private communications between users while making it harder for adversaries to focus their attacks. In this paper we first identified a number of problems and strengths in previously proposed solutions. We proposed a solution that provides stronger Anonymity properties while also solving some of the efficiency problems. We also provide an analysis of how our protocol achieves its goals.

Tracy Camp Jeff Boleng Vanessa Davies [2] Ad-hoc network protocol can vary significantly with different mobility models. Mobility model may require a data traffic pattern which significantly influences protocol performance. For instance, if a

group mobility model is simulated, then protocol evaluation should be done with a portion of the traffic local to the group. Ad hoc network protocol should be evaluated with the mobility model that most closely matches the expected real-world scenario. In fact, the anticipated real-world scenario can aid the development of the adhoc network protocol significantly. However, since the development of ad hoc networks is relatively new, we do not yet know what a realistic model is for a given scenario. In fact, we are just beginning to see realistic trace files for PCS or cellular networks.

Brad Karp and H. T. Kung [3] GPSR's benefits all stem from geographic routing's use of only immediate-neighbor information in forwarding decisions. Routing protocols that rely on end-to-end state concerning the path between a forwarding router and a packet's destination, as do source-routed, DV, and LS algorithms, face a scaling challenge as network diameter in hops and mobility increase because the product of these two factors determines the rate that end-to-end paths change. Hierarchy and caching have proven successful in scaling these algorithms. Geography, as exemplified in GPSR, represents another power full ever for scaling routing.

III. PROBLEM FORMULATION

- AESER dynamically partitions a network field into zones and randomly chooses nodes in zones
- Next relay node and uses the GPSR algorithm to send the data to the relay node.
- AESER has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity.

IV.SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

Anonymity in Mobile Ad Hoc Networks includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. "Identity and location anonymity of sources and destinations means it is hard if possible for other nodes to obtain the real identities such as ID, sequence number, routing path etc.

4.1.1 DRAWBACKS

- Public-key based encryption method is costly
- The traditional AODV protocol does not hide its locations and node ID's
- Data protection is too less
- ALERT has only prevented the data from limited level of attacks; it cannot prevent the network from all type of the network. ALERT is not completely bulletproof to all attacks.

4.2 PROPOSED SYSTEM

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Encryption secure Routing protocol (AESER). In each routing data sender partition the field into two zones. Then the packets can be transferred from and one of the zone; and elect eny one relay node for packet transmission. It uses GPSR to send the data to the relay node. At the last, the data is broadcasted to 'n' nodes in the destination zone, providing k-anonymity to the destination. The AESER hide the sender nodes packets among the number of nodes to the anonymity protection of the source.

AESER is also resilient to intersection attacks and timing attacks. We theoretically analyzed AESER in terms of anonymity and efficiency.

4.2.1 ADVANTAGES

- AESER provides route anonymity, identity, and location anonymity of source and destination
- Rather than relying on hop-by-hop encryption and redundant traffic, AESER mainly uses randomized routing of one message copy to provide anonymity protection.
- AESER can also avoid timing attacks because of its non fixed routing paths for a source destination pair.
- We conducted comprehensive experiments to evaluate AESER's performance in

comparison with other anonymous protocols

V.SYSTEM DESIGN

5.1 METHODOLOGY

Existing anonymous routing protocols relying on either hop-by-hop encryption or generates high cost. The routing protocols such as AODV do not have the methods to preserve the location identity of the nodes because it stores the every active communication route whether it is short lived or not. In proposed system using GPSR (Greedy Perimeter Stateless Routing) along with AODV. By using GPSR it is possible to hide the location information (source, destination and route) of the nodes and to ensure efficient routing in networks.

For transmitting secure data against the hacker's means not only using anonymity protection but it also needs data encryption method using DSA algorithm. So the proposed system consist routing protocol AODV for communication, GPSR for geographic location based routing algorithm, cryptographic algorithm DSA for data encryption and decryption.

5.2 SYSTEM ARCHITECTURE

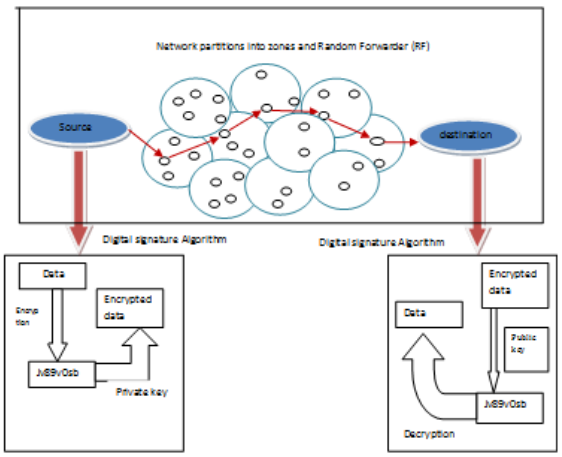

Figure 5.1: Proposed System Architecture

The source node sends the RREQ to all the nodes between the destination get RREP from available node between source and destination Each and every node sends this route request to nearby node for knowing the active node. By using AODV protocol the packet transmitted by source to destination using intermediate nodes. GPSR dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, AESER offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. DSA asymmetric cryptography algorithm is used to simulate the security properties of a signature in digital, Digital signature schemes normally has two algorithms, one for signing which involves the user's secret or private key, and one for verifying signatures which involves the user's public key.

VI.SYSTEM MPLEMENTATION

6.1 NETWORK CRATION AND ROUTING

- In this module, a Mobile Ad Hoc Networks is created in grid topology. All the nodes are configured and randomly deployed in the grid network. Since our network is a Mobile Ad Hoc Networks, nodes are assigned with mobility (movement) by using AODV.A sample routing is performed to check the connectivity in the network.

6.2 NETWORK PARTITION INTO ZONES AND HIDING LOCATION IDENTITY USING GPSR

- In this module, GPSR module is configured. A malicious node can identify the location by accessing the data packets. In this kind of routing the network is divided into non-overlapping zone and each zone is identified by a zone ID, each node in the zone is assigned a node ID. The zones have to be worked out during the design stage of the network. A node knows its physical location by using the GPSR, this information is used to map the nodes to the respective zones. AESER dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes. The zone can be divided based using simple geographic partitioning, the zone size depends on factors such as node mobility, network density, transmission power and propagation characteristics.
- The location information is added with data packets and routed to the destination. When the

destination location is not known in advance, it has to be requested by using a location service which provides a mapping from node addresses to their physical locations.

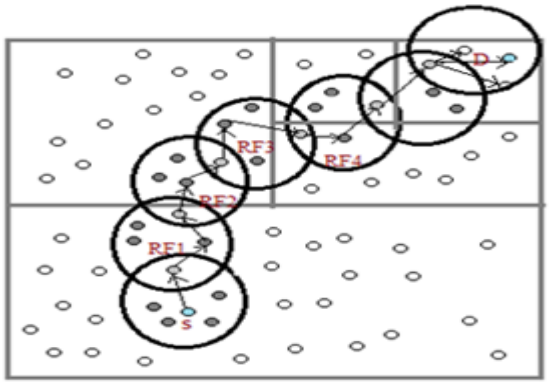

Figure 6.1 :Zone partition

6.3 THE AESER ROUTING ALGORITHM

The entire network area is generally a rectangle in which nodes are randomly disseminated. The configuration of the bottom-right and upper-left boundary of the area is configured for each node when it joins the system. AESER features a dynamic and unpredictable routing path, which consists of a number of intermediate relay nodes which is dynamic in nature. We then vertically partition zone A1 to B1 and B2. Here after, we horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner.

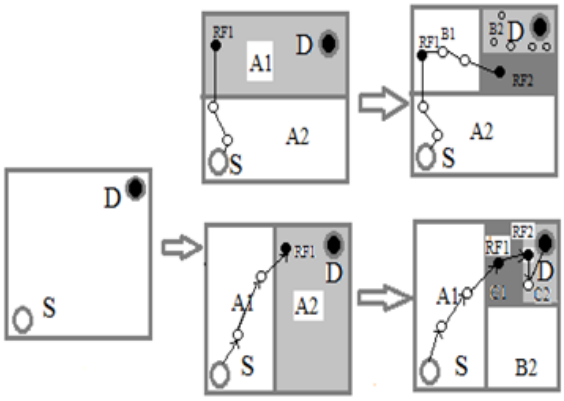

Figure 6.2: Random Forwarder

AESER uses the hierarchical zone partition which randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable path for a message. In this design, the tradeoff is the anonymity protection degree and transmission delay. A larger number of hierarchies generate more routing hops, which increases anonymity degree but also increases the delay.

4. AESER IMPLEMENTATION USING DSA

In this AESER method implemented across the network. All the nodes can hide their location information inside the data packets using AESER method.

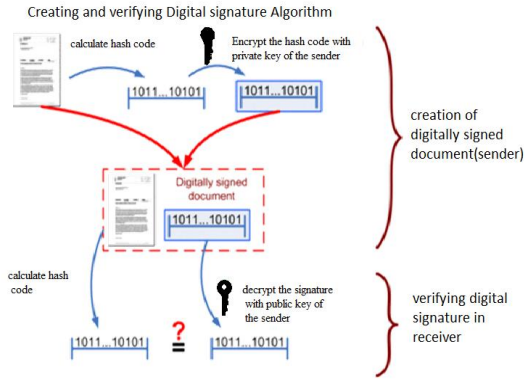

Figure 6.3 : Digital signature algorithm

VII. PERFORMANCE EVALUATION

SIMULATION PARAMETERS	
Simulator	Ns-2.34
Simulation duration	100 Seconds
Simulation Area	500*500 Sq.meters
Number of nodes	30
Transmission Range	220m
MAC Layer Protocol	IEEE 802.11
Maximum speed	5 m/s
Packet rate	8 packet per sec
Traffic Type	CBR
Data Payload	512 bytes/packet
Transmission rate	10Mb max and 3 Mb min

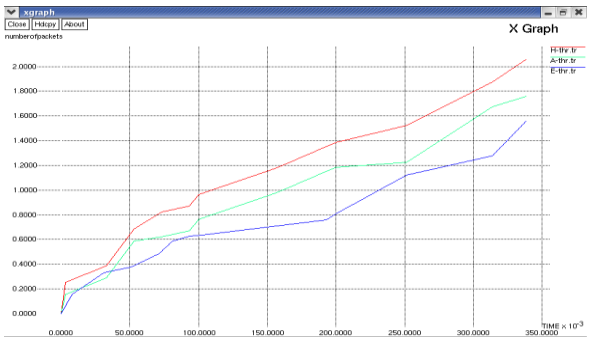

Figure 7.1: Throughput comparison

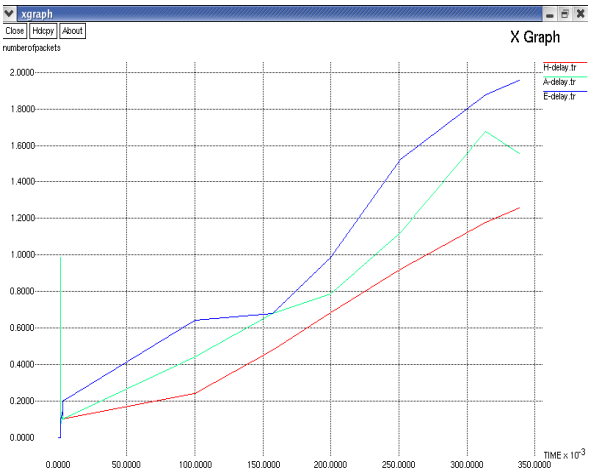

Figure 7.2 : Delay Comparison

VIII. CONCLUSION & FUTURE ENHANCEMENTS

8.1 CONCLUSION

Some protocols are unable to provide complete source, destination, and route anonymity protection. AESER is distinguished by its low cost and anonymity protection for sources, destinations, and routes. AESER has an efficient solution to counter intersection attacks. It has an ability to fight against timing attacks. Resilience to intersection attacks and timing attacks, AESER avoid timing attacks because of its non fixed routing path for a source-destination pair.

It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in AESER includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination.

8.2 FUTURE ENHANCEMENT

Furthermore, in an effort to prevent the attackers from initiating forged data attacks, we extended our research to incorporate digital signature. In future it is necessary to prevent energy loss due to the broadcasting of packets to all nodes in destination zone. AESER is not completely bulletproof to all attacks when the attackers are smart enough to packets. Future work lies in reinforcing AESER in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

REFERENCES

[1]. Brad Karp and H. T. Kung “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”.

[2]. Camp, T.,Boleng J.,Davies V.; A survey of mobility models for ad hoc network research. Wireless Communication and Mobile Computing 2(5), 483-502(2002).

[3]. Cetinkaya E.K., Broyles, D., Dandekar, A., Srinivasan, S., Sterbenz, J.P.G: Modeling Communication Network Challenges for Future Internet Resilience Survivability and Disruption Tolerance: published on line: 21 September 2011.

[4]. C.-C. Chou, D.S.L. Wei, C.-C. Jay 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, pp. 192-203, Jan. 2007.

[5]. I. Aad, C. Castelluccia, and J. Hubaux, “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Secure comm and Workshops, 2006.

[6]. J. Broch D. A. Maltz D. B. Johnson Y.C. Hu andJ. Jetcheva “A Performance Comparison of Multi_Hop Wireless Ad_Hoc Network Routing Protocols”

[7]. J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, “A Scalable Location Service for Geographic Ad Hoc Routing,” Proc. ACM MobiCom, 2000.

[8]. Perkins, ET. al. “Ad hoc On-Demand Distance Vector (AODV) routing”, RFC 3561, July 2003.

[9]. K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location-Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.

[10]. L. Zhao and H. Shen, “ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs,” Proc. Int’l Conf. Parallel Processing (ICPP), 2011.