AN EFFICIENT POSITION BASED GEOGRAPHIC ROUTING FOR ANONYMITY AND SECURITY IN MANET

[1]M.USHA, [2]P.PRITTOPAUL, [3]B.PRAVEEN KUMAR, [4]M.YAKESHRAJ

[1,2]Assistant Professor, Department of CSE, Velammal Engineering College,Chennai,India
[3,4]Department of CSE, Velammal Engineering College,Chennai,India
E-mail: [1]umahalingam@gmail.com, [2]p.prittopaul@gmail.com, [3]praveenaryadurai@gmail.com, [4]vsssrockyak@gmail.com

Abstract- Mobile Ad hoc Network (MANET) use anonymous routing protocol that hide node identities and/or routes from outside observers in order to provide anonymity protection. Some of the existing link based protocols such as Adhoc On demand Distance Vector protocol (AODV) leads to weaker security and results in performance degradation due to source trace backs. This work addresses the problem that AODV cannot achieve complete anonymity for highly dynamic mobile ad hoc networks in a secure manner. Driven by this issue, an efficient Position-based Geographic routing is proposed which takes advantage of greedy forwarding of packets to the nodes closer to the destination. Security analysis demonstrates that geographic routing can well protect user privacy against both inside and outside attackers. Geo routing uses a novel combination of group signature and id-based encryption for route recovery. Thus anonymity is preserved for source, destination and routes in a secure manner. Geo routing is implemented using Network simulator (NS-2), and evaluates its performance by comparing with AODV. The duplication results show that geographic routing has satisfactory performance compared to AODV and also achieves stronger privacy protection.

Keywords: MANET, AODV, Geographic Routing,Anonymity.

I. INTRODUCTION

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae.

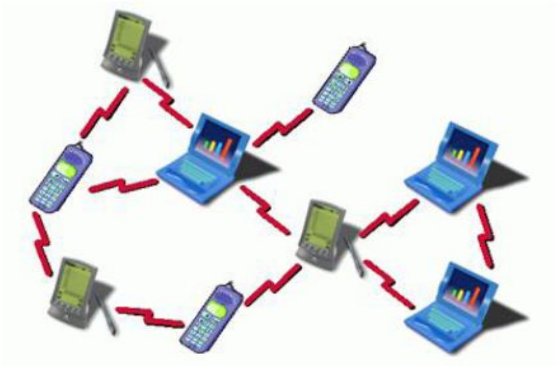


Figure 1.1 Architecture Diagram Of MANET [17]

If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their message, which effectively builds connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function excluding any statically established infrastructure or centralized administration.[17]
The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient.

1.2. CHARACTERISTICS OF MANET

- Operating without a central coordinator
- Multi-hop radio relaying
- Frequent link breakage due to mobile nodes
- Constraint resources (bandwidth, computing power, battery lifetime, etc.)
- Instant deployment

1.3. APPLICATIONS

- Military applications
- Collaborative computing
- Emergency rescue
- Mesh networks
- Wireless sensor networks
- Multi-hop cellular networks
- Wireless Community Network

1.4. MAJOR ISSUES AND CHALLENGES

- Hidden terminal problem
- Exposed terminal problem
- Channel efficiency
- Access delay and fairness
- Differential service
- Realistic mobility modeling
- Power-aware routing

II. ROUTING PROTOCOLS IN MANET:

To find and maintain routes between nodes in a dynamic topology possibly with uni-directional links, using minimum resources. Routing protocols for MANETs can be broadly classified[18] into three main categories:-

1) Proactive routing protocols(Table Driven

Routing):-Every node in the network has one or more routes to any possible destination in its routing table at any given time.

2) Reactive routing protocols(On Demand Routing):-Every node in the network obtains a route to a destination on a demand fashion. Reactive protocols do not maintain up-to-date routes to any destination in the network and do not generally exchange any periodic control messages.
3) Hybrid routing protocols:-The third class of MANET routing protocol is the hybrid protocols. It combines the advantages of both proactive and reactive routing protocols and reduces the limitations of these two. Hybrid type reduces the traffic overhead in proactive and transmission latency in reactive protocols. Every node acts reactively in the region close to its proximity and proactively outside of that region, or zone.

III. ROUTING ATTACKS IN MANET:

Attacks at the routing level can be classified into two main categories: incorrect traffic generation and incorrect traffic relaying. Sometimes these coincide with node misbehaviors that are not due to malice, e.g. node malfunction, battery exhaustion, or radio interference. Some of the attacks are :

- Flooding Attack : exhaust network resources, overall bandwidth, and individual nodes resources of computational and battery power
- Link Withholding Attack : Attacker does not advertise a link to a specific node or group of nodes
- Black hole Attack: Attacking node A returns fake routing information, causing the source node to choice a route through A, the attacker can then misuse or drop messages as it sees fit.
- Link Spoofing Attack : A attacking link advertises links to non-neighbors, by faking links to the two-hop neighbors of S, A can become one of its MPR nodes, and then manipulate traffic.
- Replay Attack : Attacker records another nodes control messages and resend them later. Can be used to spoof another node or just disrupt routing
- Wormhole Attack : Two colluding attackers have a high speed link between them. Any RREQ that pass through the colluding nodes A1 and A2 will appear to cross the shortest path because of the high-speed link. This will cause S to send all messages to D through the compromised links A1 and A2.

IV. ANONYMOUS ROUTING REVISITED

Anonymous routing protocols are essential to provide anonymity between sources to destination for data transmission. The attacker can attack or hack the data which has sent by source in different ways. There are different types of anonymous routing protocols to provide anonymity.

USOR [8] is proposed to offer complete unlinkability and content unobservability for all types of packets. USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers.

Position-based Opportunistic Routing (POR) protocol is proposed which takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. POR achieves excellent performance even under high node mobility with acceptable overhead and the new void handling scheme also works well.

ALARM [5] provides both security and privacy features, including node authentication, data integrity, anonymity, and untraceability (tracking-resistance). It also offers protection against passive and active insider and outsider attacks. This work represents the first comprehensive study of security, privacy, and performance tradeoffs in the context of link-state MANET routing.

MASR [6] **(**MANET anonymous secure routing),is inspired by a combination of DSR, TOR, ANODR and an on DSR and can overcome the limitations of current anonymous routing protocols.

Anonymous secure routing (ASR)[3] protocol is proposed that can provide additional properties on anonymity, i.e. identity anonymity and strong location privacy, and at the simultaneously ensure the security of discovered routes against various passive and active attacks.

Trust-aware routing [9] for anonymity reliable anonymous MANET routing protocol in the sense that the communicating parties are capable of choosing a secure end-to-end route free of any untrustworthy node during the anonymous route discovery process. The key features of this scheme are including of accomplishment of anonymity-related aim, trust-aware anonymous routing, effective pseudonym management and light weight overhead in computation, communication and storage.

ODAR [10], an On-Demand Anonymous Routing protocol for wireless ad hoc networks to enable complete anonymity of nodes, links and source-routing paths/trees using Bloom filters. In anonymous routing, the forwarding nodes identities are known only by the nodes themselves and no pseudonyms are necessary.

In the previous work, in any ad hoc network there is

lot of possibility for routing attacks, in which sinking is a malicious behaviour of nodes. Existing routing protocols mainly consider partial anonymity in MANET to achieve their goals. Complete anonymity is not guaranteed due to incomplete content protection. Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. unprotected packet type and sequence number also make existing schemes observable to the adversary. Until now, there is no solution being able to achieve complete anonymity and security

V. PROPOSED SYSTEM

The existing system, mainly consider partial anonymity in MANET. These Protocols support Source Trace back. Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which may lead to source trace back attacks. Meanwhile, vulnerable packet type also makes existing schemes observable to the adversary. This also results in performance degradation of networks in existing routing protocols .Until now, there is no solution being able to achieve complete anonymity in a secure manner. In the proposed system an efficient Position-based Geographic routing is implemented, which achieve complete anonymity and security by employing anonymous key establishment based on group signature. The setup is simple; each node has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme. Each packet is validated using bit validation technique, which protect all parts of a packet's content.. The intermediate node validates 4-Bit key and the destination node validates the id based group signature key .If the validation is successful by an intermediate key it can only forward the packet to the next node .Forwarded packets are encrypted using private key of an intermediate node .The forwarded packets are acknowledged by sending a beacon reply. In case if the previous node doesn't receive the beacon reply it waits for a specified holding time, then also if it doesn't receive beacon reply it retransmits the packet. With these key establishments the transmission of packets between source and destination is anonymous. Security is achieved by public key cryptography which uses decentralization method. Geo routing uses a novel combination of group signature and id-based encryption for route recovery. Fig 5.1 describes the procedure od proposed system.

Better protection against attackers is evidenced in the proposed approach. The parameters like throughput, delay, path length, packet forwarding time, packet forwarding hop are considered for comparing the performance of AODV and Geographic routing with security. Proposed to simulate and show the performance of these parameters are efficient than existing link based protocols. The results are inferred from X-graph.

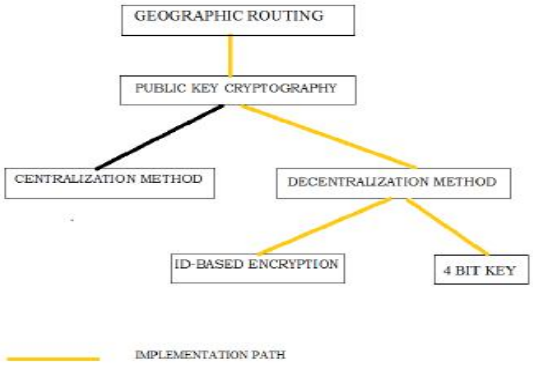


Fig.5.1 Architecture Diagram Of Proposed System.

VI. IMPLEMENTATION:

6.1. AODV Routing

On-demand routing is performed, in which the nodes are dynamic in nature. The AODV routing protocol is a reactive routing protocol .Therefore routes are determined only when needed. As data flows from the source to the destination, each node along the route updates the routes in the routing table. The routing table contains the information about source, destination and route which leads to source trace back.

Network is established in which the fields are partitioned into zones. The nodes are dynamic in nature, which move from one zone to another zone. Using the Network created, AODV protocol (link state routing) is implemented in which the transmission of packet is simulated using NS-2. In this type of protocol the node sends the packet to the neighboring node hence the path length is maximum. Moreover, the path in which the packet is transmitted from one node to another node is clearly visible for outsiders. Therefore source and destination are identified by the attackers which pave the way to discover the route in which the packet is transmitted. This indicates that the complete anonymity cannot be accomplished by the implementation of AODV in MANET. The implementation of the protocol is studied by X-graph. It is generated for the parameters like throughput, average power consumption etc. From this x-graph behavior of the protocol is clearly observed for the above parameters.

6.2. Geographic Routing

Geographic routing or position-based routing is a routing principle that relies on geographic position information. It is mainly proposed for wirelessnetworks and based on the idea that the

source sends a message to the geographic location of the destination instead of using the network address. Geo routing greedily forwards the packets. It is because the property of stateless indicates that no node in a network does not maintain any routing table. Greedy forwarding tries to bring the message closer to the destination in each step using only local information. Thus, each node forwards the message to the neighbor that is most suitable from a local point of view. The most suitable neighbor can be the one who minimizes the distance to the destination in each step (Greedy).

6.3. Geographic Routing with security

This module showsthe enhancement of previous module by adding Public key cryptosystem as a security technique. This technique is further divided into centralized and decentralized method. In this project decentralization method is used where each node can encrypt/decrypt the data and act independently. The sender node will encrypt the data with two keys namely 4-bit key and group signature. 4-bit key is decrypted by all intermediate nodes but only the destination node can decrypt the group signature. Bit validation technique is used for validating the keys. Session key, a type of private key, is established with neighbour node in transmission of packets. The above keying techniques make Geographic routing more secure than AODV protocol. This is inferred from X-graph. The graph compares both the protocol with the parameters like throughput, delay, path length etc.

CONCLUSION

In the Conclusion, Geographic routing protocol is based on group signature and ID-based cryptosystem for ad hoc networks. The design offers strong anonymity and security for ad hoc networks. The security analysis demonstrates that Geographic not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. 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.

The above parameters are taken as input for x-graph. The results observed from x-graph shows that geographic routing with security is efficient for anonymity than the existing link based protocols routes.

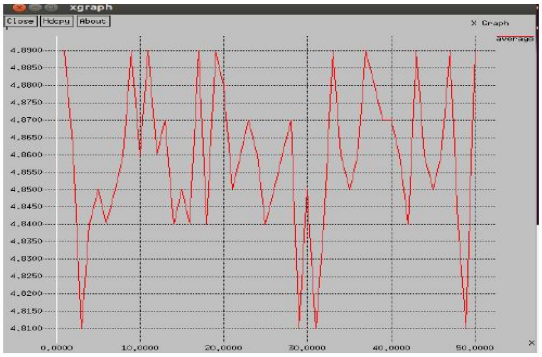
FUTURE WORK

Future work includesdeveloping an analytical model which captures the lossin node privacy due to the dynamics of the speed andthe mobility pattern of nodes inside the MANET. This work does not provide complete security to all attacks. Future work lies in reinforcing Geographic routing in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

PERFORMANCE METRIX

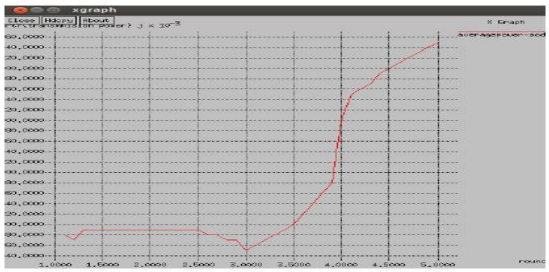
Throughput

Throughput is calculated as no of packets delivered per second. In this graph no of packets is plotted against X-axis and time is plotted against Y-axis.



Average Power

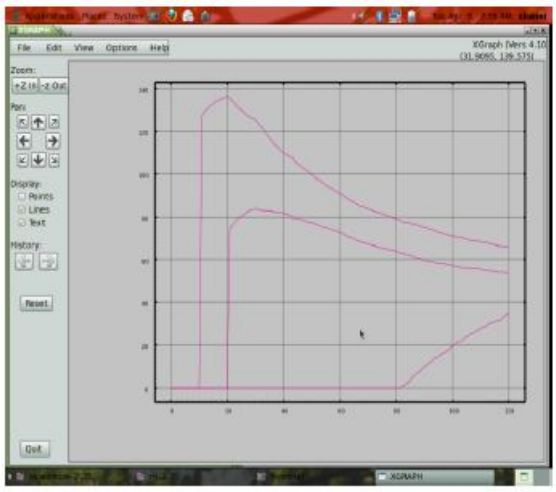
Average poweris power transmitted per time. As time increases power transmission also increases.



COMPARISON BETWEEN AODV AND SECURITY ENHANCED GEOGRAPHIC ROUTING

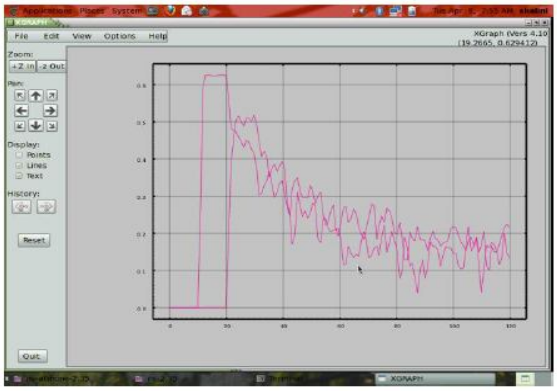
a. Delaying

Due to the local key construction delay result in longer latency of Geo Routing than AODV.



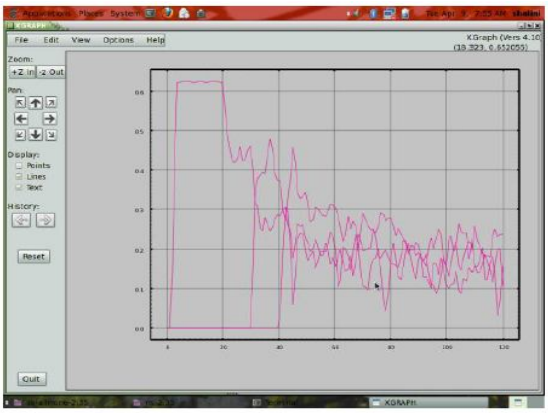
b. Packet forwarding by time

AODV has the highest packet delivery ratio for both types of traffic loads the packet delivery ratio decreases as the nodal speed increases and traffic load become heavier. Under the light traffic load geo routing has more than 90% packet delivery ratio .under the heavy traffic load geo routing performance decreases as the node speed increases.



c. Throughput

The below graph Shows the throughput of receiving packets vs simulation time in that manner slightly increase in simulation of throughput receiving packets in simulation time of 300 sec.It is observed that throughput is better than AODV by 37.5%.



REFERENCES

[1] Shengbo Yang, Chai Kiat Yeo ,Lee "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks" IEEE Trans. Mobile Comput., vol. 11, no. 1, pp. 10.1109/TMC.2011.55

[2] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108

[3] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE ternational Conference on Advanced Information Networking and Applications, pp. 133–137

[4] L. Song, L. Korba, and G. Yee, "An anonymous secure routing protocol for mobile ad hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33– 42

[5] K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011

[6] JunPan, JianhuaLiMASR" An Efficient Strong Anonymous Routing Protocol for Mobile Adhoc Networks "IEEE Trans. Mobile Comput., vol. 11, no. 1, pp 10.1109/ICMSS.2009.5301090

[7] Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624

[8] Zhiguo Wan ,KuiRen, Ming Gu" USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE Trans. Mobile Comput., vol.10,no.11,pp.1345–1358

[9] Min-HuaShao,Shin-Jia Huang "Trust Enhanced Anonymous Routing in Mobile Ad-Hoc Networks" IEEE Trans. Mobile Comput., vol. 11, no. 1, pp10.1109/PDCAT.2008.10

[10] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[11] "http://www.isi.edu/nsnam/ns" accessed on December 24, 2012

[12] "http://mohittahiliani.blogspot.in/" accessed on February 20, 2013

[13] "http://mohittahiliani.blogspot.in/2010/08/xgraph-and-awk-scripts-in-ns-2_06.html" accessed on March 17, 2013

[14] "https://www.google.co.in/#output=search&sclient=psy-ab&q=ns2+installation" accessed on January 10, 2013

[15] "http://www.google.com/geographicrouting" accessed on February 14,2013

[16] "http://mohittahiliani.blogspot.in/2009/12/awk-script-for-ns2.html" accessed on March 3,2013

[17] "http://www.google.co.in/search?q=mobile+ad-hoc+network&sa=X&hl=en&tbm=isch&tbo=u&source=univ&ei=Jf9vUezVJ83rrQej4YDIDA&ved=0CDwQsAQ&biw=1600&bih=775#imgrc=p-by2PdR7ctOpM%3A%3Bdu-6rFnO3CtIpM%3Bhttp%253A%252F%252Fwww.ece.iupui.edu%252F~dskim%252Fmanet%252Fimages%252Fadhocnet.gif%3Bhttp%253A%252F%252Fwww.ece.iupui.edu%252F~dskim%252Fmanet%252F%3B541%3B385" accessed on March 20, 2013

[18] Routing techniques for Mobile Ad Hoc Networks Classification and Qualitative/Quantitative Analysis, by Mr. AnkurKhetrapal,Delhi University.

★★★