ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

Efficient Anonymous Multicast Routing Protocol in MANET

V.Madhumitha[#1], Dr. S. Kirubakaran[*2]

[#] M.E, Department of Computer Science and Engineering, Info Institute of Engineering, Coimbatore, Tamil-Nadu, India

[*] Assistant Professor, Department of Computer Science and Engineering, Info Institute of Engineering, Coimbatore, Tamil-Nadu, India

ABSTRACT: Mobile Adhoc Networks are infrastructure less networks and the topology of the network changes dynamically. The dynamic change in topology leads to malicious traffic analysis. Inorder to provide security from malicious attackers, anonymous protocols are used. An anonymous protocol hides the nodes identity and path involved in the data transfer.

The proposed Anonymous multicast routing (AMR) scheme provides anonymous protection with less delay and it blocks the malicious nodes which are involved in the data transfer prior to the transmission of the data. For efficiency and reliability, the data packets are divided into segments and the segments are transferred through multiple paths.

KEY WORDS: Anonymous, Multicast routing, Delay, Efficiency.

I.INTRODUCTION

Rapid deployment of independent mobile users will be the need of the next generation wireless communication systems. A mobile ad-hoc network is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Network scenarios which include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. Network topology changes rapidly and unpredictably over time due to the mobility of the nodes [9], [10], [11]. To protect wireless communication, many security protocol suites have been designed and deployed. But, they do not give significance to anonymity protection and leave mobile nodes to be traceable by wireless traffic analysts.

A. Anonymity:

Anonymity is an important issue in electronic payments and electronic voting, electronic auctions, email and web browsing. Anonymity [12] is the state of being not identifiable within a set of subjects, the anonymity set.

I. Data anonymity:

Data anonymity is filtering any identifying information out of the data that is exchanged in a particular application.

II. Connection anonymity:

Connection anonymity is hiding the identities of source and destination during the actual data transfer.

Connection anonymity is only considered in this context. The concept of anonymity is defined in terms of either Unlinkability or Unobservability. Network transmissions are considered as the items of interest (IOIs). The difference between Unlinkability and Unobservability is whether security protection covers Items of Interests or not.

III. Unlinkability:

Anonymity in terms of Unlinkability is defined as Unlinkability of an IOI and a pseudonym. An anonymous IOI is not linkable to any pseudonym, and an anonymous pseudonym is not linkable to any IOI.

IV. Unobservability:

Unobservability also protects IOIs from being exposed. That is, the message transmission is not discernible from random noise.

B. Necessity of Anonymity in MANET:

Concept of anonymity has recently attracted attention in mobile wireless security research. Proactive routing and global-knowledge-based routing schemes are the ones used in infrastructure networks to provide anonymity protection. These are not applicable in the case of mobile ad hoc networks. Mobile nodes are traceable by methods which were infeasible in infrastructure networks. In hostile environments, the adversary can launch traffic analysis against intercept able routing information in routing messages and data packets. This should be prevented to make sure that active attacks do not take place. Route anonymity and location privacy are the two addressed issues to be handled by the anonymous routing protocol.

C. Attackers:

Passive attackers may be universal in a hostile environment. However, an attacker with unbounded computing capability and active interference capability is capable of crushing any practically implemented security protocol. Thus, the routing schemes are so designed so as to be secure against powerful attackers with unbounded eavesdropping capability but bounded computing and node intrusion capability. An attacker can be at two levels.

1. Level of link intrusions.

2. Level of node intrusions.

The proposed Multicast routing scheme solves both link and node intrusions. The proposed scheme provides anonymous protection with less delay and increases the packet delivery ratio. Efficiency and reliability of the network can be increased by considering multiple paths. By considering multiple paths retransmission of packets will take less time.

II. RELATED WORK

Y.V.S.Sai pragathi et.al [2] uses both proactive and reactive mode of anonymous location based routing. Proactive mode is applicable to the nodes within the predefined radius and this involves construction of topology tables of the nodes. Reactive mode is applicable for the nodes outside the predefined radius and this involves route discovery process by broadcasting route request message and getting route reply from the intermediate nodes. Group head node is selected in the network on the basis of maximum connectivity. Building topology table is difficult in mobile networks. This technique reduces the delay when compared to other anonymous protocols.

Javier Campos's et.al [3] proposed a protocol HOP and implemented it and it is based on cryptographic Host Identity Protocol (HIP) which offers security and user level anonymity. Some enhancement is done to the authentication process to achieve Host Identity Tag (HIT). HIP protocol is combined with OLSR routing protocol to achieve the support for pseudonym. It uses multiple IP addresses per station (one per destination) to achieve a higher degree of anonymity when communicating. When two nodes wish to establish a secure connection, each will select a free IP address from its IP address pool that is used as a pseudonym for that connection. This approach is lightweight and it is easy to implement. It maximizes the performance. The maximum data encryption rate was limited to 12 M bit/s.

Simardeep Kaur et.al [4] proposed a method of routing protocol using GPS**.** Hybrid protocols are used which combines the advantages of both reactive and proactive protocols. Position-based routing thus does not require the establishment or maintenance of routes. Location services can be classified according to how many nodes host the service. The position information can be collected in different ways .It can be collected from the direction and strength of the received wireless signals and through interfacing with a low-power Global Positioning System (GPS) and a satellite updating the positions of the nodes by sending signals to this GPS device. It has disadvantages like the problem of designing location update schemes to provide accurate destination information.

K. Sanzgiri et.al [5] proposed the Authenticated Routing for Ad hoc Networks. (ARAN) protocol uses public key cryptography instead of the shared security association. Each intermediate node running this protocol verifies the integrity of the received message before sending it to its neighbour nodes. The transmitting nodes rely on the use of certificates included in the route discovery and reply messages in order to authenticate each other. Alternatively, certificates can cost money, limiting the ability of the attackers to request them limitlessly. A short lifetime on certificates can also help manage the network. The protocol has an optional second discovery stage that provides non-repudiating route discovery.

Yih-Chun Hu et.al [6] proposed a scheme based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to protect from Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network resources or processing time, an efficient one-way hash function is used and asymmetric cryptographic operations is not used in this protocol. SEAD performs well over the range of scenarios tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node; it performs well even in spite of any active attackers or compromised nodes in the network.

Xiaoyan Hong et.al [7] presents a survey of various mobility models in both cellular networks and multi-hop networks. The group motion of nodes occurs frequently in ad hoc networks, and based on this group motion, a novel group mobility model – Reference Point Group Mobility (RPGM) is introduced, it represent the relationship among mobile hosts. RPGM can be readily applied to many existing applications. Moreover, by proper choice of parameters, RPGM can be used to model several mobility models which were previously proposed. One of the main themes of this approach is to investigate the impact of the mobility model on the performance of a specific network protocol or application. To this end, RPGM model to two different network protocol scenarios, clustering and routing, and have evaluated network performance under different mobility patterns and for different protocol implementations. In conclusion, when the mobility of the node increases, the overhead also increases. This shows that the mobility of the nodes affects the performance. Delay and packet delivery ratio depends upon the mobility of the nodes. Mobility nodes cannot be determined accurately.

III. PROPOSED SYSTEM

A. Networks, Attack Models and Assumptions:

The proposed routing scheme can be applied to network models with different node movement patterns such as random way point model and group mobility model. A communication protocol which provides anonymous protection should provide Untraceability. Untraceability is needed to ensure the sender's anonymity, when the sender communicates with the other side of the network. Moreover, a malicious observer or eavesdroppers may try to block the data packets by compromising the nodes in the network, and also intercept the packets on a number of nodes, or even trace back to the sender by detecting the direction of the data transmission. Therefore, the route should also be undetectable. Anonymous routing protocols should provide undetectable routes that transfer the data. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity.

B. Attackers:

The attackers may be of two types.

First can be battery powered nodes that passively receive network packets but not change the contents and detect activities in their vicinity and also detect the traffic flow pattern.

The second can be powerful nodes that are active attackers that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets. They change the contents of the packet. The assumptions below apply to both inside and outside attackers.

1. Capabilities: These passive attackers tend to observe the flow of the packets through a path. By eavesdropping, the attacker nodes can analyze any routing protocol that is used and obtain information about the communication packets in their vicinity and positions of other nodes that communicate with each other in the network. They can also monitor data transmission when a node is communicating with other nodes and can record the historical information about the communication between the nodes. By using the historical information they start attacking. They also control the behaviour of other nodes, e.g., with denial-of-service (DoS) attacks, which may affect the routing in existing anonymous geographic routing methods.

2. Incapability's: The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period.
Therefore, encrypted data are secure to certain degree when the key is not known to the attackers.

C. Location Service and Dynamic Pseudonym:

When two nodes want to communicate, the source node S sends a request to a destination node D and the destination responds with data. A transmission session is the time period that S and D interact with each other continuously until they stop. For each transmission session the different pseudonym is used. Each node uses a dynamic pseudonym [1] as its node identifier instead of its real MAC address, which can be used to trace nodes' presence in the network. To calculate the pseudonym, collision resistant hashes function, such as SHA-1 is used, to hash a node's MAC address and current time stamp. Inorder to prevent an attacker from calculating the pseudonym, the time stamp should be small (e.g., nanoseconds). Considering the network delay, it takes 105 times to the attacker for one packet per node. The attacker needs to observe many nodes to compute the pseudonym, so the computing overhead is very high and it is not in the acceptable range, and the success rate is also too low. To further make the attackers work difficult to calculate the times tamp, the computation complexity can be increased by using randomization for the time stamps. Specifically, we keep the precision of time stamp to a certain extent, say 1 second, and randomize the digits within 1/10th. Thus, the pseudonyms cannot be easily reproduced. A node's pseudonym expires after a specific time period (for a single data transmission) in order to prevent adversaries from associating the pseudonyms with nodes. The pseudonyms should not be changed too frequently, because the routing will get disturbed; and if pseudonyms are changed too infrequently, the adversaries may associate pseudonyms with nodes across pseudonym changes. Therefore, the pseudonym change should be appropriately determined. Each node periodically updates its updated position and pseudonym to "hello" messages, and sends the messages to its neighbours. Also, every node maintains a table with routing information that keeps its neighbours' pseudonyms associated with their locations.

D. Anonymous Routing Protection (ARP):

The number of node in the network can be allocated according to the need. The source and the destination node are determined. Each node in the network knows the position of its neighbours. When the node moves from its position, the distance between those two nodes gets updated. In order to reduce the delay involved in the data transfer the intermediate node with minimum hop should be selected. Before the data gets transmitted, the intermediate nodes which will be involved in the transfer of the data packets will be determined. It is determined by considering the minimum hop distance. The other node in the network does not know about the selected path and about the data transfer through the selected path. Thus the data transmission achieves anonymous protection. Attacker cannot perform link level intrusion or cannot attack a targeted path or a route. In order to protect the data from the selfishness nodes or attacker nodes in the selected path a separate method is used.

If delay increases in the selected path or when the nodes have no battery to transfer the packet an alternative path should be selected. In case of an attacker node in the selected path, it increases the delay and consumes the energy of the nodes. In these cases the alternate path is selected and the data is transferred. The attacker node does not know about the new path selection.

In summary,
1. Anonymous routing: It provides route anonymity, and location anonymity of source and destination.
2. Low cost: Rather than relying on hop-by-hop encryption and redundant traffic, it mainly uses randomized routing of one message copy to provide anonymity protection.
3. Resilience to intersection attacks and timing attacks: It has a strategy to effectively counter intersection attacks, which have proved to be difficult. It can also avoid timing attacks by relaying on random routing paths for a source destination pair.
4. Extensive simulations: We conducted comprehensive experiments to evaluate the performance.

The routing scheme contributes to the achievement of anonymity by restricting a node's view only to its neighbours present in the selected path and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source or a forwarding node.

The problem of dead end [1] is common in all the geographic routing protocol. In a network all the nodes are aware of the position of its neighbour node in order to forward a packet to the neighbour node which is nearest to the destination. A dead end problem occurs when a packet is forwarded to a node whose neighbours are all further away from the destination than itself and then the packet is routed between neighbours iteratively. This iterative forwarding of the packets between the neighbour nodes is the dead end problem. The proposed system can overcome the problem of dead end, without compromising anonymity protection.

E. Anonymous Multicast Routing (AMR):

The network area is divided into zones. The zones should be of equal size. Group member is selected in each zone.

I. Zone Management:

The zone head manages the nodes in those zones. Nodes join and leave a zone by sending "join" and "leave" packets to the zone head. Join and leave packets are multicast packets with destination lists that contain only the zone head address. In the case of nodes joining or leaving, the zone head must send "update" packets including a list of its updated multicast zone members to all zone nodes. Nodes send "join" packets periodically to the zone head, and nodes that die without sending" leave" packets are removed from the list after a time-out period. The zone head manages the routing information and the zone heads of all the zones are involved in finding the minimum hop between the source and the destination. Position verification tests are done to the zones. Reference Point zone member mobility model is used to model zone mobility. Each zone has a logical "centre" called a reference point and zone members (nodes).

II. Direct symmetry test:

In the Direct Symmetry Test [8], S verifies the direct links with its communication neighbours. To this end, it checks
1. Reciprocal Time of Flight-derived distances are consistent with each other.

$| d_{s\,x} – d_{x\,s}|>2e_r+e_m$

2. The position advertised by the neighbour.

$| ||p_{s}\text{-}p_{x}||\text{-}d_{s\,x}|>2e_p+e_r$

3. The proximity range R.

$D_{s\,x>R}$

The nodes for the data transfer are selected. Once the nodes for the data transfer are selected, malicious nodes in order obtain the data that is transferred, may compromise the selected node. If the selected node is compromised, then it starts obtaining the data that is transferred. To prevent this attack, prior to the data transfer direct Symmetry test is performed. The result of the test is returned to the group member of the respective zone. The group members will multicast the result to all other members in that zone. Then the malicious or attacker node is blocked and it cannot be involved in the data transfer. Thus the anonymous protection is obtained.

III. Multiple Paths:

Mobile Ad Hoc Networks (MANETs) are comprised of highly mobile nodes that communicate with each other without relying on a pre-existing network infrastructure. Due to their applications in situations such as emergencies, crisis management, military and healthcare, message security is of paramount importance in mobile ad-hoc networks. However, because of the absence of a fixed infrastructure with designated centralized access. A misbehaving node can abide well in the route discovery phase and hence be placed on utilized routes. Inorder to provide protection from misbehaving nodes many methods can be used. Multipath routing consists of finding multiple routes between a source and destination node. These multiple paths can be used to compensate for the dynamic and unpredictable nature of ad hoc networks. The data packets when transferred through single path, retransmission during packet loss takes more time. Inorder to improve the efficiency and reliability the data packets are divided into segments and transmitted through different paths. When the data packets are transmitted through multiple paths ,the attacker cannot obtain the whole data and also it takes only less time for retransmission of lost packets.

IV.SIMULATION RESULTS

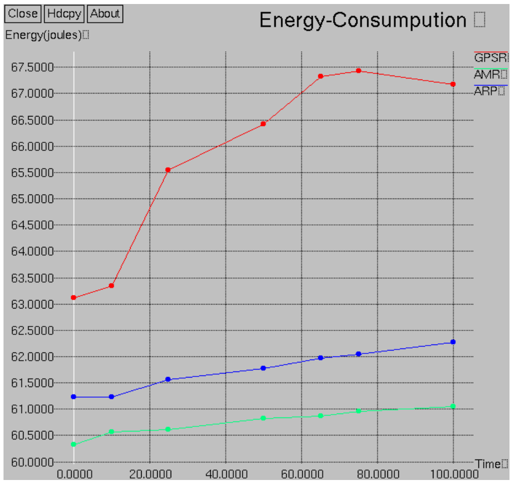

Figure1: Comparision of energy consumption between GPSR, ARP and the proposed AMR protocol.

Figure 1 shows that the energy consumption reduces for the proposed AMR scheme when compared to GPSR and ARP.

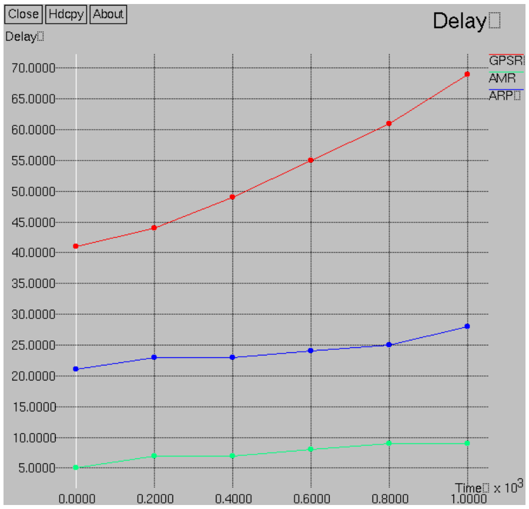

Figure2: Comparision of delay between GPSR, ARP and the proposed AMR protocol.

Figure 2 shows that the delay decreases for the proposed AMR scheme when compared to GPSR and ARP.

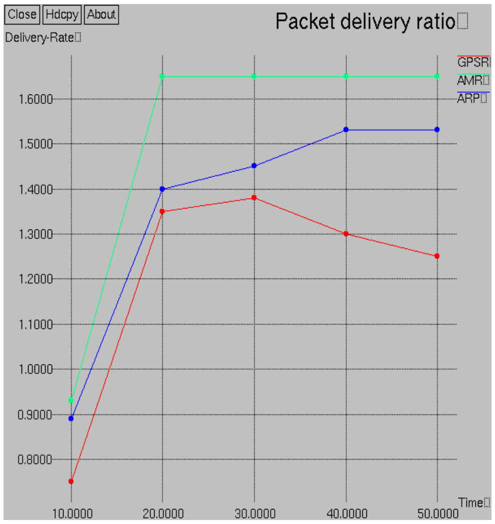

Figure3: Comparision of packet delivery ratio between GPSR, ARP and the proposed AMR protocol.

Figure 3 shows that the packet delivery ratio increases for the proposed AMR scheme when compared to GPSR and ARP.

V.CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. They did not consider the delay involved in the transfer of the data. When the destination node moves faraway from its position during the transfer of the packet, the delay increases. The proposed AMR scheme block the malicious nodes prior to the transfer of the data packets, once the malicious nodes are blocked they will not be involved in any transfer. The proposed AMR scheme is reliable, efficient as it sent the data through multiple paths. Thus the proposed AMR scheme is efficient.

REFERENCES

[1] Haiying Shen, Lianyu Zhao,"ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" IEEE Transactions On Mobile Computing, Vol.12, No. 6, JUNE 2013.

[2] Y.V.S.Sai pragathi, S.P. Setty," Hybrid Anonymous Location-Aided Routing Protocol For Privacy Preserving And Authentication In Manet", Journal of Theoretical and Applied InformationTechnology,Vol.55No.2,20thSeptember2013

[3] Javier Campos, Carlos T. Calafate,Marga N´acher, PietroManzoni, and Juan Carlos Cano," HOP: Achieving Efficient Anonymity in MANETs by Combining HIP, OLSR, and Pseudonyms", Hindawi Publishing Corporation EURASIP Jour on Wireless Communications and Networking Volume 2011, Article ID 437868, 14 pages, 1 September 2010.

[4] Simardeep Kaur, Anuj K. Gupta," Position Based Routing in Mobile Ad-Hoc Networks", IJCST Vol. 3, Issue 4, Oct - Dec 2012.

[5] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M.A Belding- Royer," A Secure Routing Protocol For Ad Hoc Networks", in: Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November,2002.

[6] Yih-Chun Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[7] Z.Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 2006.

[8] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos," Discovery and Verification of Neighbour Positions in Mobile Ad Hoc Networks" IEEE Transactions On Mobile Computing, Vol. 12, No. 2, FEBRUARY 2013

[9] G.Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Computing. Science, vol. 3, no. 8, pp. 574–582, 2007.

[10] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[11] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron, vol. 57, no. 3, pp. 840–849, Mar. 2010.

[12]A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.