LOCATION TRUST EXTENDED AUTHENTICATION IN MOBILE AD HOC NETWORKS

[1]P.Kanmani, [2]K.Krishnan
[1]PG Scholar, Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri
[2]Assistance Professor, Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri
[1]kanmanisasi1989@gmail.com

Abstract: Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic, either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications. To offer high anonymity protection at a low cost, we propose an Anonymous Location-based Efficient Routing protocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.

Keywords: Mobile ad hoc networks, anonymity, routing protocol, geographical routing.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing.

Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-byhop encryption and redundant traffic For example, ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and only focuses on destination anonymity. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR).In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing protocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route.

1.1 Anonymous routing

ALERT provides route anonymity, identity, and location anonymity of source and destination.

1.2 Low cost

Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.

1.3 Resilience to intersection attacks and timing attacks

ALERT can also avoid timing attacks because of its non-fixed routing paths for a source destination pair.

1.4 Extensive simulations. We conducted comprehensive experiments to evaluate ALERT's performance in comparison with other anonymous protocols.

2. ALERT: AN ANONYMOUS-LOCATION BASED EFFICIENT ROUTING PROTOCOL

2.1 Networks and Attack Models and Assumptions

ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility model.

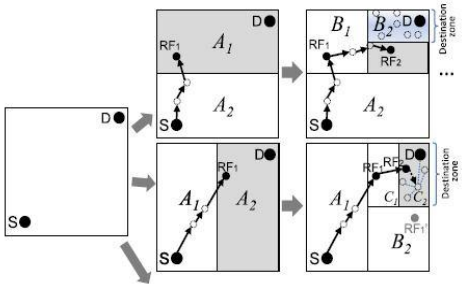

Figure 1: Examples of different zone partitions

2.2 The ALERT Routing Algorithm

ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. As shown in the upper part of Fig. 1, given an area, we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. We call this partition process hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relaynode (i.e., data forwarder), thus dynamically generating un predictable routing path for message.

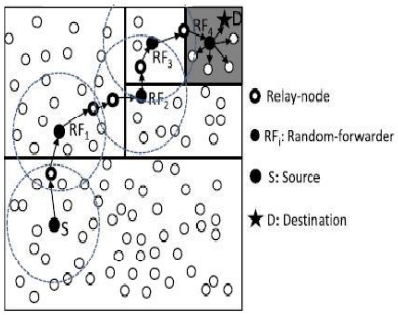

Figure 2: Routing among zones in ALERT

Zone having k nodes where D resides the destination zone, denoted as ZD. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 2 is the destination zone. Specifically, in the ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and ZD are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF).

ALERT aims at achieving k-anonymity for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in ZD, providing k-anonymity to the destination. Given an S-D pair, the partition pattern in ALERT varies depending on the randomly selected TDs and the order of horizontal and vertical division, which provides a better anonymity protection. Fig. 1 shows two possible routing paths for a packet pkt issued by sender S targeting destination D in ALERT. There are also many other possible paths. In the upper routing flow, data source S first horizontally divides the area into two equal-size zones, A1 and A2, in order to separate S and ZD. S then randomly selects the first temporary destination TD1 in zone A1 where ZD resides. Then, S relies on GPSR to send pkt to TD1. The pkt is forwarded by several relays until reaching a node that cannot find a neighbor closer to TD1. This node is considered to bethe first random-forwarder RF1. After RF1 receives pkt, it vertically divides the region A1 into regions B1 and B2 so that ZD and itself are separated in two different zones. Then, RF1 randomly selects the next temporary destination TD2 and uses GPSR to send pkt to TD2. This process is repeated until a packetreceiver finds itself residing in ZD, i.e., a partitioned zone is ZD having k nodes. Then, the node broadcasts the pkt to the k nodes.

3. ANONYMITY PROTECTION AND STRATEGIES AGAINST ATTACKS

This section discusses the performance of ALERT in providing anonymity protection and its performance and strategies to deal with some attacks.

3.1 Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing which always takes the shortest path, ALERT makes the route between an SD pair difficult to discover by randomly and dynamically selecting the relay nodes. The resultant different routes for transmissions between a given SD pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, his detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

3.2 Resilience to Timing Attacks

In timing attacks, through packet departure and arrival times, an intruder can identify the packets transmitted between S and D, from which it can finally detect S and D.

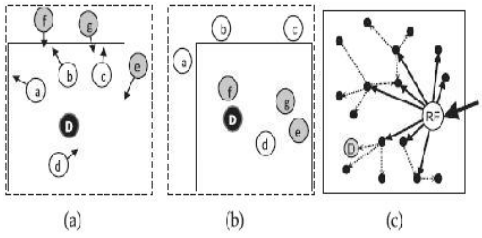

Figure 3: Intersection attack and solution

For example, two nodes A and B communicate with each other at an interval of 5 seconds. After a long observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33,20:01:38). Then, the intruder would suspect that A and B are communicating with each other. Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In ALERT, the "notify and go" mechanism and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to intruders. More importantly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps anintruder from identifying the S and D.

3.3 Strategy to Counter Intersection Attacks

In an intersection attack, an attacker with information about active users at a given time can determine the sources and destinations that communicate with each other through repeated observations. Intersection attacks are a well-known problem and have not been well resolved. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in ZD during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the destination zone except D.

As a result, D is identified as the destination because it always appears in the destination zone. Fig. 3a is the status of a ZD after a packet is broadcasted to the zone. The arrows show the moving directions of nodes. We can see that nodes a, b, c, d, and D are in ZD. Fig. 3b is the subsequent status of the zone the next time a packet is transmitted between the same SD pair. This time, nodes d, e, f, g, and D are in ZD. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker watches the process, the easier it is to identify the destination node. To counter the intersection attack, dynamically enlarges the range of anonymous zones to broadcast the messages or minimizes communication session time. However, the former strategy increases the communication overhead, while the latter may not be suitable for long duration communication. Instead of adopting such a mitigating mechanism, we propose another strategy to resolve this problem. Note that the attacker can be puzzled and lose the cumulated observation by making it occasionally fail to observe D's reception of packets. Since packets are delivered to ZD constantly in longduration sessions rather than using direct local broadcasting in the zone, the last RF multicasts packet pkt1 to a partial set of nodes, say m nodes out of the total k nodes in the zone. The m nodes hold the packets until the arrival of the next packet pkt2.Upon the arrival of the next packet; the m nodes conduct one-hop broadcasting to enable other nodes in thezone to also receive the packet in order to hide D.Fig. 3c shows the two-step process with the first step in solid arrows and the second step in

dashed arrows. We can see that the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of pkt1 and pkt2 are mixed, an attacker observes that D is not in the recipient set of pkt1 though D receives pkt1 in the delivery time of pkt2.Therefore, the attacker would think that D is not the recipient of every packet in ZD in the transmission session, thus foiling the intersection attack. Because the attacker may grab and analyze packets on air, the last forwarding node alters a number of bits in each packet to prevent the attacker from identifying identical packets in one broadcasting. The Bitmap records the altered bits and is encrypted using the destination's public key KD pub for recovering the original data. Since destination is not always within the recipient set, and the packet forwarded to adestination is different from the original packet, the attacker cannot identify the destination from its observation history by calculating the intersection set of nodes. This approach incurs two extra costs. One is the on hop broadcasting of the recipients in the destination zone. The other is the encryption cost of changed bits.

4. RELATED WORKS

Anonymous routing schemes in MANETs have been studied in recent years. By the different usage of topological information, they can be classified into on-demand or reactive routing methods and proactive routing methods. Also there are anonymous middleware working between network layer and application layer. Since topology routing does not need the node location information, location anonymity protection is not necessary. Hop-by-hop encryption and redundant traffic routing in hop-byhop encryption routing, a packet is encrypted in the transmission of two nodes en route, preventing adversaries from tampering or analyzing the packet contents to interrupt the communication or identify of the two communicating nodes. Hop-by-hop encryption routing can be further divided into onion routing and hop-by-hop authentication. In onion routing, packets are encrypted in the source node and decrypted layer by layer (i.e., hop by hop) along the routing path. It is used in Aad , ANODR and Discount-ANODR topological routing. Both route discovery and return routing, generating high cost. Hop-by-hop authentication is used to prevent adversaries from participating in the routing to ensure route anonymity topological routing uses neighborhood authentication in routing path discovery to ensure that the discovered routes consist of legitimate nodes and are anonymous to attackers. The works in are based on geographic routing. In GSPR, nodes encrypt their location updates and send location updates to the location server. However, GSPR does not provide route anonymity because packets.

5. FUTURE WORK

The proposed work is carried on the extension of ALERT routing. A group signature concept of key server management is introduced to provide a secure and authenticated data transmission in the mobile network in addition to ALERT algorithm. Source encrypt the data using the public key of destination, then destination request a key server to provide a private key for decrypting the encrypted data. The key server provides a private key only after verification from source node. Group signatures can be viewed as traditional public key signatures with additional privacy features. In a group signature scheme, any member of a potentially large and dynamic group can sign a message thereby producing a group signature.

A group signature can be verified by anyone who has a copy of a constant length group public key. A valid group signature implies that the signer is a bonafide group member. However, given two valid group signatures it is computationally infeasible to decide whether they are generated by the same (or different) group members. However, if a dispute arises over a group signature, a special entity called a Group Manager can force open a group signature and identify the actual signer. A mobile node can periodically sign its current location (link state) information without any fear of being tracked, since multiple group signatures are not linkable. At the same time, anyone can verify a group signature and thus be assured that the signer is a legitimate MANET node through Location Announcement Message (LAM).

5.1 ADVANTAGES

- The proposed work provides more secure data transmission in mobile network and also it can act as a resistant to certain typesof attacks.
- The delay is reduced and results in the fastest data delivery across the networks

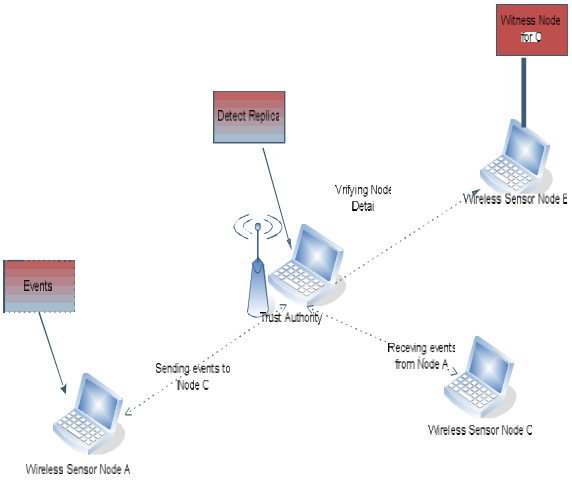

Figure 4: System Architecture

6. IMPLEMENTATION

6.1 NODE CREATIING

This module is developed to node creation and more than 50 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

6.2 ZONE PARTITION

ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. ALERT uses the hierarchical zone partition and 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 routing path for a message. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner.

6.3 DATA ROUTING

After the hierarchical zone partition process, the source and destination claimed to be in different zones. The source node sends the data to destination through the intermediate relay nodes. The user data gram protocol is used to transfer the data routing from one relay node to next relay node.

6.4 ALERT WORKING PROCESS

The main objective of the ALERT algorithm is to provide a security to the MANET by means of trust extended authentication mechanism. The ALERT setup a temporary destination TD and informs to all mobile nodes in the network, so that the attacker concentrates only on TD to hack the data. By means of diverting the attacker's concentration the data from source is delivered to original destination in secure manner.

6.5 KEY SERVER MANAGEMENT

The extended technique or proposed technique of ALERT is key server management. ALERT mechanism doesn't suitable for heavier traffic condition since ALERT is a light weight trusting mechanism. So in order to overcome this issue key server management technique is proposed. Through KSM (key server management) technique provides a more authentication and secure transmission than ALERT mechanism through data encryption and decryption technique.

6.6 ALGORITHM

Let L -1 = n* 160 + b, where both b and n are integers and $0 \leq b < 160$.

Step 1.Choose an arbitrary sequence of at least 160 bits and call it SEED. Let g be the length of SEED in bits.

Step 2. Compute U = SHA-1[SEED] XOR SHA-1[(SEED+1)mod2g].

Step 3. Form q from U by setting the most significant bit (the 2159 bit) and the least significant bit to 1. In terms of Boolean operations, q = U OR 2159 OR 1. Note that 2159< q <2160.

Step 4. Use a robust primality testing algorithm to test whether q is prime 1.

Step 5. If q is not prime, go to step 1.

Step 6. Let counter = 0 and offset = 2.

Step 7. For k = 0... n let Vk = SHA-1[(SEED + offset + k) mod 2g]. 1 A robust primality test is one where the probability of a non-prime number passing the test is at most 2-80

Step 8. Let W be the integer W = V0 + V1* 2160 + ... + Vn-1* 2(n-1)* 160 + (Vn mod 2b) * 2n* 160and let X = W + 2L-1 . Note that $0 \leq W < 2L-1$ and hence $2L-1 \leq X < 2L$.

Step 9. Let c = X mod 2q and set p = X -(c -1). Note that p is congruent to 1 mod2q.

Step 10. If p < 2L-1 , then go to step 13.

Step 11. Perform a robust primality test on p.

Step 12. If p passes the test performed in step 11, go to step 15.

Step 13. Let counter = counter + 1 and offset = offset +n+1.

Step 14. If counter ≥ 212 = 4096 go to step 1, otherwise (i. e. if counter < 4096) go to step 7.

Step 15. Save the value of SEED and the value of counter for use in certifying the proper.

7. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. 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 ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity.

ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks.

REFERENCES

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

[2] PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

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

[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] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[7] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[8] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.

[9] Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.

[10] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and

[11] Simulation of Wireless and Mobile Systems (MSWiM), 1999.