Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.249 – 253

RESEARCH ARTICLE

Mitigating Location Attacks through Trust Based Model in MANETS

SAI MIDHILA[1], G ARULKUMARAN[2], K PRABHAKAR[3]

Student, Information Technology, Vivekanandha College of Engineering for Women, TamilNadu, India[1]

Assistant Professor Department of Information Technology Vivekanandha College of Engineering for Women Tiruchengode, Erode[2]

Assistant Professor Department of Information Technology Vivekanandha College of Engineering for Women Tiruchengode, Erode[3]

saimidhus@gmail.com[1]

erarulkumaran@gmail.com[2]

k.prabhakar86@gmail.com[3]

ABSTRACT

Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols which rely on either hop-by-hop encryption or redundant traffic 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. ALERT mechanism offers anonymity protection to sources, destinations, and also routes. It has strategies which effectively help to counter intersection and timing attacks. To offer high security protection at a low cost, we propose a Trust Based Model through Recommendation and local information of neighboring node for Efficient Routing based on this ALERT. Trust model dynamically partitions the nodes into benign and suspicious based on the data transmission of neighboring node and also it mitigates the network attack through formation of intermediate relay nodes, which form a non-traceable anonymous route. It hides the data initiator/receiver among many initiators/receivers to strengthen the source and destination anonymity protection.

Keywords

Mobile ad hoc networks; anonymity; routing protocol; trust based model

1. INTRODUCTION

MANET is Mobile Ad hoc Networks in which every single node can make establish the connection and communicate with other nodes. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Here the radio waves only carry the signal between the mobile nodes. It is a wireless network and uses multi-hop peer-to-peer routing instead of static network infrastructure to provide network connectivity. MANETs have their applications in rapidly deployed and

dynamic military and civilian systems. Due to a lack of infrastructure support, each node acts as a router, forwarding data packets for other nodes. This wireless structure easily can make in anywhere.

The network topology in a MANET usually changes with time. The routers are free to move randomly and organize themselves arbitrarily and thus the wireless topology of the network may change rapidly and unpredictably. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymity may not be a requirement in civil oriented applications but it is critical in military applications. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources and destinations, as well as route anonymity.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate high cost. Many approaches cannot provide all of the aforementioned anonymity protections. The existing protocols like ALARM cannot protect the location anonymity of source and destination, another like SDDR cannot provide route anonymity, and also ZAP only focuses on destination anonymity. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR)) that greedily forwards a packet to the node closest to the destination. The protocol's relay node selection makes it easy to reveal the source and destination and to analyze traffic. Complex routing and stringent channel resource constraints of MANET impose strict limits on the system capacity. The recent increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency. However, the anonymous routing protocols which are mentioned above and other existing protocols generate a significantly high cost, and this exacerbates the resource constraint problem in MANETs. In a MANET, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations. So in order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing proTocol (ALERT) has been introduced.

ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes. This forms a non-traceable anonymous route. In each of the routing steps, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. The next relay node is randomly chosen by them which can be any node in the other zone and uses the GPSR algorithm to send the data to the relay node. Finally the data is broadcasted to k nodes in the destination zone by providing k-anonymity to the destination. ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is resilient to intersection attacks and timing attacks.

To offer high security protection at a low cost, a Trust Based Model through Recommendation and local information of neighboring node for efficient routing based on this ALERT mechanism has been proposed. Trust model dynamically partitions the nodes into benign and suspicious based on the data transmission of neighboring node and also it mitigates the network attack through formation of 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.

2. AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL (ALERT) - THE EXISTING SYSTEM

ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility model. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. Exposing the transmission direction reveals the location of a message's sender. Hence, an anonymous communication protocol that can provide untraceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. The route should also be undetectable as a malicious observer may try to block the data packets by compromising a number of nodes, intercepting packets on a number of nodes, or trace back to the sender by detecting the data transmission direction. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. In such a way the destination node also needs the protection of anonymity.

In ALERT, each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address as it can be used to trace nodes' existence in the network. We use a collision-resistant hash function, such as SHA-1, to hash a node's MAC address and current time stamp in order to avoid pseudonym collision. The time stamp should be precise enough to prevent an attacker from recomputing the pseudonym. ALERT features a dynamic and unpredictable routing path and it 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. Each data source or forwarder executes the hierarchical zone partition in the ALERT routing. It first checks whether the destination and itself are in the same zone. If it is found so, it then divides the zone alternatively in the horizontal and vertical directions. This process is repeated by the node until itself and the destination zone, denoted as ZD, is not in the same zone. After this, it then randomly chooses a position in the other zone called temporary destination (TD), and to send the data to the node closest to TD it uses the GPSR routing algorithm. 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). In the last step, the data are broadcasted to k nodes in ZD and this provides k-anonymity to the destination. The zone partitioning sample is been shown in the Figure 1.

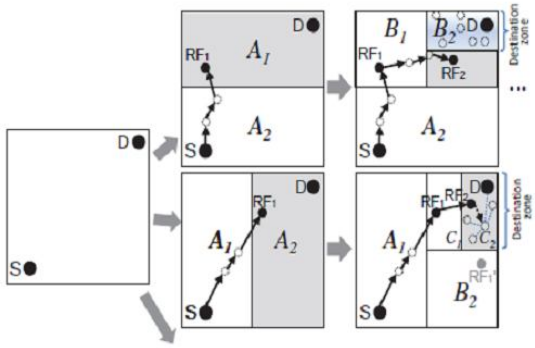

Figure 1. Samples of completely different zone partition

ALERT contributes to the achievement of anonymity by restricting a node's view only to its neighbors and constructing the same initial and forwarded messages. So this makes it difficult for an intruder to tell if a node is a source or a forwarding node. Like other anonymity routing algorithms, the existing ALERT mechanism is also not completely bulletproof to all attacks. Hence we propose a Trust based model on ALERT to thwart the attackers and make the network more secure.

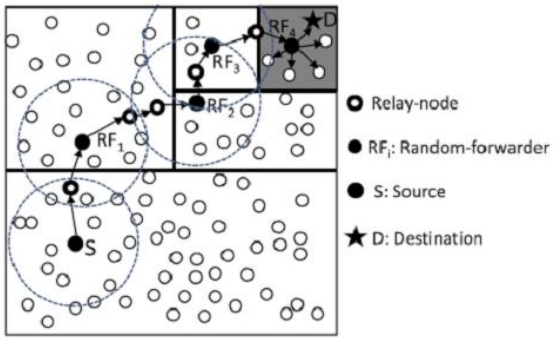

Figure 2. Routing among zones in ALERT

3. THE PROPOSED SYSTEM

We propose a Trust Based Model through Recommendation and local information of neighboring node for efficient routing based on this ALERT mechanism to offer high security at a low cost. Trust model dynamically partitions the nodes into benign and suspicious based on the data transmission of neighboring node and also it mitigates the network attack through formation of intermediate relay nodes that form a non traceable anonymous route. This also hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection.

3.1 Trust Based Model Using Recommendation Exchange Protocol

Trust is defined as a set of relations among entities that participate in a protocol. The relations are based on the evidence generated by the previous interactions of entities within a protocol. Hence in general, if the interactions have been faithful to the protocol, then we can say that trust will accumulate between these entities. Trust has also been defined as the degree of belief about the behavior of other entities (or agents). The Recommendation Exchange Protocol (REP) allows nodes to exchange recommendations about their neighbors. Thus the recommendation exchange protocol builds a trust relationship between nodes in an ad hoc network. Here the trust is based on previous individual experiences and on the recommendations of others. The basic idea is to use the period of time the recommender node knows the target node as a metric to calculate the weight of its recommendation. Humans are able to know each other better as time goes by and the same idea applies here. Nodes increase the weight of the recommendations coming from older neighbors and decrease the weight of recommendations coming from new neighbors.

Our Trust based model consists of four modules by which we are implementing our system on the ALERT mechanism. The modules are:

- A Trust level Evaluation.
- The First Trust Assignment.
- Recommendation Computation.
- The Recommendation Exchange Protocol.

3.1.1 A Trust level evaluation

The trust level evaluation is defined from node about another node as a weighted sum of its own trust and the recommendations of neighbors. The ranges from [0, 1] is the aggregate value of the recommendations from all other neighbors. The variables that ranges from [0, 1] is a parameter in our model that allows nodes to choose the most relevant factor. Where [0] means the least reliable node and [1] means the most reliable node.

3.1.2 The First Trust Assignment

We divide the trust scheme in two distinct phases. In the initial phase, nodes first meet and assign a trust level to each other. The second phase is the trust level update, which assumes that the nodes have already met each other. When a node first meets a neighbor, it assigns an initial level of trust to his neighbor. We classify the first trust assignment strategy as Prudent or Optimistic. In prudent strategy the node does not trust strangers and considers that every new neighbor as a possible threat to the network. As a consequence, the node assigns a low value of trust for the new neighbor. On the other hand, Optimistic strategy assumes that every node is reliable until proven otherwise. Here the node associates a high level of trust for new neighbors.

3.1.3 Recommendation Computation

The trust level calculation considers there commendation of neighbors obtained by the Recommendation Exchange Protocol (REP). Here at first a node defines a set which is a subset of its neighbors comprising all nodes whose trust level is a certain threshold, to increase the confidence of recommendation. The recommendation is defined as the weighted average of the recommendation from all nodes about that certain node. The Recommendation considers not only the trust level of other nodes, but also the accuracy and the relationship maturity.

3.1.4 The Recommendation Exchange Protocol

This protocol allows nodes to exchange Recommendation among them and only considers interactions with neighbors, which significantly simplifies the protocol. When using IP to broadcast the message, the Time to Live (TTL) field is set to 1. The protocol is composed of three messages:

- Trust Request (TREQ) message,
- Trust Reply (TREP) message and
- Trust Advertisement (TA) message

4. CONCLUSION

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate high cost. Many approaches cannot provide all of the aforementioned anonymity protections. In a MANET, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations. So in order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing proTocol (ALERT) has been used. But this also does not provide full network security. Mechanisms which thwart the network and security attacks should be introduced. This made the choice of proposing a Trust based system which mitigates the location and other network attacks makes the network more secured. Trust evaluation is done and with this trust value for each node, every node sends and receives the information. The Recommendation Exchange protocol is been used in order to exchange recommendations among the nodes which are the neighbors. Thus our system helps to thwart the attacks in the network layer by using a trust level based protocol. This provides source, destination and route anonymity with a low cost than other anonymous routing protocol.

5. ACKNOWLEDGMENTS

Our thanks to the almighty god, our experts and friends who have contributed towards development of the paper and for their innovative ideas.

REFERENCES

[1] Artz D and Gil Y, “A survey of trust in computer science and the semantic web," Web Semantics: Science, Services Agents World Wide Web, vol. 5, no. 2, pp. 58-71, June 2007.

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

[3] Kong J, Hong X, and Gerla M, “ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks,” Proc. ACM MobiHoc, pp. 291-302, 2003.

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

[5] Sk.Md.M. Rahman, Mambo M, Inomata A, and Okamoto E, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” Proc. Int’l Symp. Applications on Internet

[6] Velloso P. B, Laufer R. P, Duarte O. C. M. P, and Pujolle G, "Analyzing a human-based trust model for mobile ad hoc networks," in IEEE Symp. Comput. Commun., Marrakech, Morocco, July 2008.

[7] Wu X, Liu J, Hong X, and Bertino E, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[8] Yang L, Jakobsson M, and Wetzel S, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

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

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

