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 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

An Anonymous Authentication and Secure Communication Protocol in Ad-hoc Networks

D. Pavun Kumar[1], Mr S.Sundar Raj [2] M.Tech.,

M.E II Year, Department of CSE, Sri Subramanya College of Engineering and Technology, Palani, 624 615,India[1]

Assistant Professor, Department of CSE, Sri Subramanya College of Engineering and Technology, Palani, 624 615, India[2]

ABSTRAC - 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 Authentication and Secure Communication Protocol in Ad-hoc Networks (AAASCPN). AAASCPN dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, AAASCPN offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. We theoretically analyze AAASCPN in terms of anonymity and efficiency. Experimental results exhibit consistency with the theoretical analysis, and show that AAASCPN achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, AAASCPN achieves comparable routing efficiency to the GPSR geographical routing protocol.ss

KEYWORDS: MANET, High Anonymity, AAASCPN, Geographical routing protocol, Rc4 Algorithms, protection.

I. INTRODUCTION

Rapid development of 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. 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. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage. 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 (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 and exact locations of the sources and destinations. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination (i.e., relationship unobservability [1]), it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

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 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. RELATED WORK

1. Anonymous routing AAASCP provides route anonymity, identity, and location anonymity of source and destination. 2. Low cost. Rather than relying on hop-by-hop encryption and redundant traffic, AAASCP mainly uses randomized routing of one message copy to provide anonymity protection. 3. Resilience to intersection attacks and timing attacks. AAASCP has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue [16]. AAASCP can also avoid timing attacks because of its nonfixed routing paths for a source destination pair.4. Extensive simulations. We conducted comprehensive experiments to evaluate AAASCP's performance in comparison with other anonymous protocols.

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

Alert can be applied to different network models with various node movement patterns such as random way point model [17] and group mobility model [18]. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable. 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. In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets. The assumptions below apply to both inside and outside attackers.

B. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs

In many traditional mobile network scenarios, nodes establish communication on the basis of persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. Instead, nodes need to communicate on the basis of nothing more than their current locations. In this paper, we address some interesting issues arising in such MANETs by designing an anonymous routing framework (ALARM). It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and untraceability (tracking-resistance). It also offers resistance to certain insider attacks.

III. MODELS AND ASSUMPTIONS

A . Zone Partition:

This Module we can divide the network into set of zones. In this zone can communicate the different zone in the network.

B. Source Node Encryption and Random Forward Selection:

The source node protection and encryption then random forwarder can choose the randomly in the node.then transmit the data.

C. Relay Node Selection:

The relay node forwarded the next zone in the network. This can forward the data.

D. Routing Table:

The routing table can update the routing path. It can attach the time stamp. The routing table frequently changed.

E. Destination Node Decryption and Verification:

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 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The destination node receives the data and decrypts the content. it can be verified.

IV. OUR PROPOSED SCHEME

A. Main Idea

AAASCPN features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes, 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 v 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.

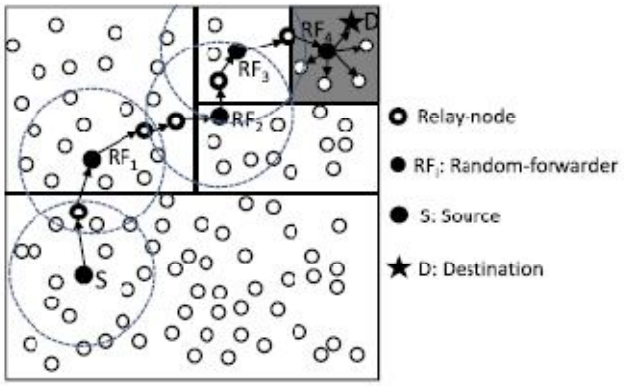

Fig. 1 The An Anonymous Authentication and Secure Communication Protocol in Ad-hoc Networks

V. DETAILS OF THE PROPOSED FRAMEWORK

We compare AAASCPN with two recently proposed anonymous geographic routing protocols: AO2P and ALARM which are based on hop-by-hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare AAASCP with the baseline routing protocol GPSR in the experiments. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination. In ALARM, each node periodically disseminates its own identity to its authenticated neighbors and continuously collects all other nodes' identities. Thus, nodes can build a secure map of other nodes for geographical routing. In routing, each node encrypts the packet by its key which is verified by the next hop en route. Such dissemination period was set to 30 s in this experiment. The routing of AO2P is similar to GPSR except it has a contention phase in which the neighboring nodes of the current packet holder will contend to be the next hop. This contention phase is to classify nodes based on their distance from the destination node, and select a node in the class that is closest to destination.

AAASCPN contributes to the achievement of anonymity by restricting a node's view only to its neighbors 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. To strengthen the anonymity protection of the source nodes, we further propose a

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 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

lightweight mechanism called "notify and go." Its basic idea is to let a number of nodes send out packets at the same time as S in order to hide the source packet among many other packets.

"Notify and go" has two phases: "notify" and "go." In the first "notify" phase, S piggybacks its data transmission notification with periodical update packets to notify its neighbors that it will send out a packet. The packet includes two random back-off time periods, t and t0. In the "go" phase, S and its neighbors wait for a certain period of randomly chosen time 2 ½t; t þ t0_ before sending out messages. S's neighbors generate only several bytes of random data just in order to cover the traffic of the source. T should be a small value that does not affect the transmission latency. A long t0 may lead to a long transmission delay while a short t0 may result in interference due to many packets being sent out simultaneously. Thus, t0 should be long enough to minimize interference and balance out the delay between S and S's farthest neighbor in order to prevent any intruder from discriminating S. This camouflage augments the privacy protection for S by _-anonymity where _ is the number of its neighbors. Therefore, it is difficult for an attacker to analyze traffic to discover S even if it receives the first notification.

AAASCPN utilizes a TTL field in each packet to prevent the packets issued in the first phase from being forwarded in order to reduce excessive traffic. Only the packets of S are assigned a valid TTL, while the covering packets only have a TTL ¼ 0. After S decides the next TD, it forwards the packet to the next relay node, which is its neighbor based on GPSR. To prevent the covering packets from being differentiated from the ones sent by S, S encrypts the TTL field using KRN pub obtained from the periodical "hello" packets between neighbors. Every node that receives a packet but cannot find a valid TTL will try to decrypt the TTL using its own private key. Therefore, only NRN will be able to successfully decrypt it, while other nodes will drop such a packet,

VI. PERFORMANCE MEASURES

1. The number of actual participating nodes. These nodes include RFs and relay nodes that actually participate in routing. This metric demonstrates the ability of AAASCPN randomized routing to avoid routing pattern detection.
2. The number of random forwarders. This is the number of actual RFs in a S-D routing path. It shows routing anonymity and efficiency.
3. The number of remaining nodes in a destination zone. This is the number of original nodes remaining in a destination zone after a time period. A larger number provides higher anonymity protection to a destination and to counter the intersection attack. We measure this metric over time to show effectiveness on the destination anonymity protection.
4. The number of hops per packet. This is measured as the accumulated routing hop counts divided by the number of packets sent, which shows the efficiency of routing algorithms.
5. Latency per packet. This is the average time elapsed after a packet is sent and before it is received. It includes the time cost for routing and cryptography. This metric reflects the latency and efficiency of routing algorithms.
6. Delivery rate. This is measured by the fraction of packets that are successfully delivered to a destination. It shows the robustness of routing algorithms to adapt to mobile network environment.

VI. 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 An Anonymous Authentication and Secure Communication Protocol in Ad-hoc Networks (AAASCPN) 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 AAASCPN includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. AAASCPN 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. In addition, ALERT has an efficient solution to counter intersection attacks. AAASCPN ability to fight against timing attacks is also analyzed. Experiment results show that AAASCPN 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, AAASCPN is not completely bulletproof to all attacks. Future work lies in reinforcing AAASCPN in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results

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 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

REFERENCES

[1] 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.
[2] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs,"Proc. Int'l Conf. Parallel Processing (ICPP),2011.
[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.
[5] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007