Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

Research Paper

Security Analysis and Provide Trust Extended Authentication Using Group Signature

Computer Science

KEYWORDS : Mobile ad hoc networks, zone partition, group signature

Ms. Reshna Wilson Department of Computer Science,Nehru Instituite of Technology, Coimbatore

Mr. Biju Balakrishnan Department of ComputerScience,Nehru Institute of Technology,Coimbatore

ABSTRACT

Security and protection of private user information are a prerequisite for the deployment of the mobile network technologies.Nevertheless, the establishment of secure communication architecture within mobile ad hoc networks addresses special challenges, due to the characteristic and specific cities of such environment (high dynamic and mobility of nodes, high rate of topology changes, high variability in nodes density and neighbourhood, broad- cast/geocast communication nature). . A number of secure authentication schemes based on asymmetric cryptography have been proposed to prevent such attacks. In this paper, we address some interesting issues arising in such MANETs by designing an anonymous routing framework (ALERT) extended to key server management and group signature algorithm. It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other relay nodes it wants to communicate with. ALERT 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.

1 INTRODUCTION

Security has became an important concern in order to provide protected communication between mobile nodes Mobile Ad-hoc network is one of the most promising fields for research and development of wireless networks. As the Ad –hoc network technology has become widespread vulnerabilities in its security issue/problem are increasing which can be dangerous to the privacy of the user's personal information. The complexity and uniqueness of MANETS make them vulnerable to security threats. Attacks on ad hoc wireless networks can be classified as passive and active attacks ,depending on whether the normal operation of the network is disrupted or not. Providing security in MANET is a challenge that needs to be approached at different levels .MANETS and their self configuring mobile routers are vulnerable due to their wireless connectivity and their frequent topology changes. Ad –hoc networks are new networks for the wireless communication

In this paper, we address some interesting issues arising in such MANETs by designing an anonymous routing framework (ALERT) extended to key server management and digital signature algorithm. It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other relay nodes it wants to communicate with. ALERT 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.The ALERT protocol is a light weight protocol, so it does not provides a heavy authentication against adversary attacks. Due to its nature there could be a delay in transmitting data. And also the ALERT protocol does not satisfy the network constraints in larger network with more number of mobile nodes. So in order to overcome this issue a new protocol to be implemented extended to ALERT protocol. Simply future work concentrates on providing more authentication and reducing the work load. It provides a more security to the mobile network. Due to its importance the key exchange algorithm is proposed to implement in mobile network in order to provide a heavy data authentication and to reduce the work load. By extending the team protocol we can provide a secure data authentication even in the presence of adversary attackers.

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).

My paper is organized as follows: The next section (Section

2) gives you an idea of the current and existing methods in the assurance of security. Section 3 gives the proposed schema used. Then I conclude the paper in the following section. Last section is fully dedicated to the papers which I have refereed to make do my research work.

[2]RELATED WORKS

Ad hoc Network Using Alarm:

Proposed by S Karthiga and V.B.Rosy Christiana." (2012) privacy in Suspicious Mobile In this paper they had reviewed the alarm protocol for mutual authentication .The Alarm protocol is to ensure data integrity and confidentiality .In Alarm protocol two approaches are there of group digital signature and link state routing The link protocol is for maintain link between mobile nodes and group signature to digitally sign the message to ensure message integrity and confidentiality The message is encrypted by the public key which is announced group manager and every group manager is having their private keys .to ensure digital signature group manager is responsible.[9].

Other research results have yielded anonymous on-demand routing protocols, such as SPAAR , ASR , MASK , ANODR . These protocols use pseudonyms for node identification and addressing but none of them utilizes location information for routing. Location-based routing protocols mainly focus on improving the performances of the routing protocol and minimizing overhead by utilizing location information to deliver routing con-trol messages in MANETs without flooding the whole network.

Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

Mix zones and GLS are zone-based location services.
A Mix zone is an anonymous location service that unveils the positions of mobile users in a long time period in order to prevent users' movement from being tracked. Each location aware application that can monitor nodes' locations on top of Mix zones is only allowed to monitor the nodes that are registered to it. Therefore, by letting each node associate with some zones but stay unregistered, these users' location changes are untraceable in unregistered zones. Although GLS also uses hierarchical zone partition-ing, its use is for location service while in ALERT, its use is for anonymous routing. ALERT is also different from GLS in the zone division scheme. A zone in ALERT is always divided into two smaller rectangles, while GLS divides the entire square area into four sub squares and then recursively divides these into smaller squares. The zone division in ALERT occurs when selecting a next forwarding node, so the zones are formed dynamically as a message is being forwarded. In contrast, the zone division and hierarchies in GLS are configured in advance and the location servers are selected based on the different hierarchies.

A Group Mobility Model for Ad Hoc Wireless Networks
In this a survey of various mobility models in both cellular networks and multi-hop networks.We show that group motion occurs frequently in ad hoc networks, and introduce a novel group mobility model Reference Point Group Mobility (RPGM) - to represent the relationship among mobile hosts. RPGMcan 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 paper is to investigate the impact of the mobility model on the performance of a specific network protocol or application. To this end, we have applied our 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. As expected, the results indicate that different mobility patterns affect the various protocols in different ways. In particular, the ranking of routing algorithms is influenced by the choice of mobility pattern.

[3] ALERT: AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL

A. 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 [11] and group mobility model [1]. 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 proto-col 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. 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.

B.NODE CREATION
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.

C.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

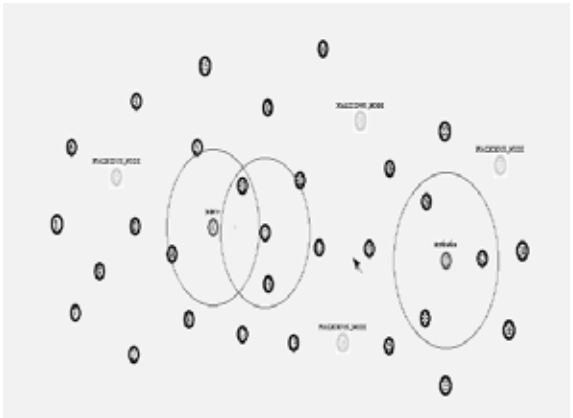

FIG 1.Zone Partition

D.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.

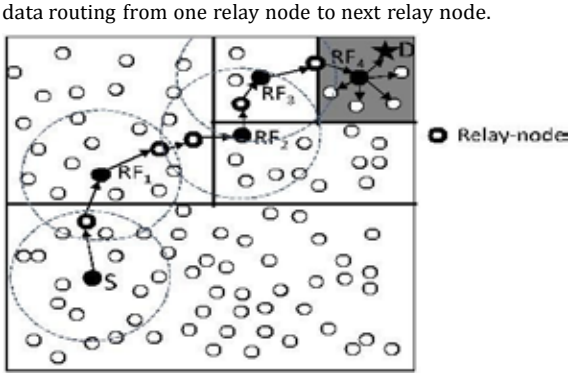

FIG.2. Routing among zones

E.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.

FIG 2.Performance level on routing

[4]. GROUP SIGNATURE TECHNOLOGY

roup signature[1] schemes are an important building block for many security applications. In contrast to ordinary signature schemes where there is only one signer, group signature schemes allow any member of a group of signers to sign documents on behalf of the group. In general, a group manager controls the group membership and issues group signing keys to group members. The group signing keys allow a group member to sign documents on behalf of the group. In particular, a group signature scheme provides anonymity and unlinkability to the signer, i.e. everybody can verify that the signature is valid on behalf of a group, but nobody except for the group manager can identify the signing member. Furthermore it is computationally hard for anybody but the group manager to decide whether two different valid signatures were generated by the same group member. These attractive security properties make group signature schemes appealing to applications such as electronic voting, electronic auctions and many applications where it is desirable to hide organizational structure. Group signature schemes are also used in electronic cash systems to conceal the cash-issuing banks' identities and identity escrow systems.

A group signature scheme consists of the following four procedures:

SETUP: a probabilistic interactive protocol between a designated group manager and the members of the group. Its result consists of the group's public key Y, the individual secret keys x of the group members, and a secret administration key for the group manager.

SIGN: a probabilistic algorithm which, on input a message m and a group member's secret key x, returns a signature s on m. VERIFY: an algorithm which, on input a message m, a signature s, and the group's public key Y, returns whether the signature is correct.

OPEN: on input a signature s and the group manager's secret administration key this algorithm returns the identity of the group member who issued the signature s together with a proof of this fact.

It is assumed that all communications between the group members and the group manager are secure.

[5]. KEY SERVER MANAGEMENT

The extended technique or proposed technique of A LERT 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] .CONCLUSION

In this paper, states a packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination by means of temporary destination. ALERT further strengthens the anonymity protection of source and destination by KEY SERVER MANAGEMENT (KSM) hiding the data initiator/receiver among a number of data initiators/ receivers. And also tried to present various types of attacks on group signature and requirements for this technique.

REFERENCE

[1] [1] D. Boneh and H. Shacham. Group signatures with verifier- local revocation. In V. Atluri, B. Pfitz-mann, and P. D. McDaniel, editors, ACM Conference on Computer and Communications Security, ACM, 2004. | | [2] [2]J. Camenisch and M.Stadler, "Efficient group signature scheme for large groups", in Advances in Cryptology, Crypto 1997 | | [3] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN),2004. | | [4] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW),2004. | | [5] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. | 1297-1309, Oct. 2008. | | [6] 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. | | | | [7] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L.Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, 2003. | | [8] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobserva-bility (WDIAU), pp. 10-29, 2001. | | | | [9] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002. | | [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 Simulation of Wireless and Mobile Systems (MSWiM), 1999. | . | |