Mobile Ad Hoc Network Security Issues

Tejashree Kokate
ME 2nd year student
MMCOE, Karve Nagar
Pune

Ram Joshi
Head of Department
MMCOE, Karve Nagar
Pune

ABSTRACT
This paper studies mobile Ad hoc network technology uses and how it can be used in real life applications. As now a day's lots of Research is going on automotive vehicles, if mobile ad hoc network is used to represent vehicles on roads and vehicle to vehicle communication is made possible then travelling will be easy and enjoyable. Due to mobile nature and scalability in mobile ad hoc networks anyone in the network can communicate anytime anywhere.

This paper gives quick overview of existing technologies in MANETs.

General Terms
Network security, security issues in mobile ad hoc network, securing MANETs, vehicular communication system, vehicle to vehicle communication using MANETs, dynamic network security

Keywords
MANET based vehicular communication security issues, Securing mobile ad hoc network, vehicle to vehicle communication protocol, VNETs security issues

1. INTRODUCTION
In today's digitized world, information exchange has become essential. If some new technology proves useful somewhere and catches limelight then it spreads everywhere. If we look back 10 years back use of mobiles, GPS like technologies were used only by rich and educated people. But over the period of time they have become affordable and easy to use. Microprocessors and wireless adapters embedded in many devices, as cell-phones, PDAs, Laptops, digital sensors, and GPS receivers allow such easy to use devices. These well-equipped devices have made wireless mobile networks available at most of the places and both together are today giving more attractive applications.

Some applications of mobile networks are still "under construction". As example of such applications can be emergency disaster relief after a storm or an earthquake, vehicle to vehicle communication in daily life where drivers can't make time to communicate they are rushing to the destination. Other examples of such applications are, Exchange of control messages in polymer industry, a military tanks and planes in a battle who want to exchange information. Infrastructure independency has become a key point in much such application's development. This Infrastructure independency requirement leads to a new kind of mobile network; ad hoc networks.

A mobile ad hoc network, or MANET, is a temporary infrastructure less network, formed by a set of mobile nodes which dynamically establish their own network without any central administration.

2. SECURITY REQUIREMENTS OF A NETWORK
The security services of ad hoc networks are similar to network communication paradigms[6]. Focus is on protecting the information and the resources from attacks. Also misbehavior should also be taken care off. Minimum requirements of security paradigm are:

Availability: It ensures that the desired network services are available whenever they are expected, irrespective of attacks. System that ensures availability removes denial of service and energy starvation attacks.

Authenticity: It ensures communication from one node to another is genuine. It ensures that there is no malicious node that can masquerade as a trusted network node.

Data confidentiality: It is security primitive for ad hoc networks that ensures if given message cannot be understood by anyone else than its (their) desired recipient(s). Data confidentiality is typically enabled by applying cryptography.

Integrity: It denotes the authenticity of data sent from one node to another. That is, it ensures that a message sent from node A to node B was not modified by a malicious node, C, during transmission.

If a robust confidentiality mechanism is employed, ensuring data integrity may be as simple as adding one-way hashes to encrypted messages.

Non-repudiation ensures that the origin of the message is legitimate. i.e. when one node receives a false message from another, non-repudiation allows the former to accuse the later of sending the false message and enables all other nodes to know about it. Digital signature is used to ensure non-repudiation.

3. MANET FEATURES
The features of MANETs make them more vulnerable to attacks and misbehavior than traditional networks, and impose the security solution to be different from those used in other networks. These features are

Infrastructure less: Central servers, specialized hardware, and infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships.

That is, they assume contributory collaborative roles in the network rather than ones of dependence. i.e., any security solution should rely on cooperative scheme instead of centralized one.

Wireless links use: The use of wireless links renders a wireless ad hoc network susceptible to attacks. Unlike wired networks where an adversary must gain physical

access to the network wires or pass through several lines of defense at gateways, attacks on a wireless ad-hoc network can come from all directions and target at any node. Hence, a wireless ad hoc network will not have a clear line of defense, and every node must be prepared to threats. Moreover, since the channel is widely accessible, the MAC protocols used in ad hoc networks, such IEEE802.11, rely on trusted cooperation in a neighborhood to ensure channel access, which presents vulnerability.

Multi-hop: Because the lack of central routers and gateways, hosts are themselves routers, then packets follow multi-hop routes and pass through different mobile nodes before arriving to the destination. Because of the possible untrustworthy of such nodes, this feature presents a serious vulnerability.

Nodes movement autonomy: mobile nodes are autonomous units that are capable of roaming independently. This means that tracking down a particular mobile node in a large scale ad hoc network cannot be done easily.

Amorphous: Nodes mobility and wireless connectivity allow nodes to enter and leave the network spontaneously. Therefore, the network topology has no form regarding both the size and the shape.

Hence, any security solution must take this feature into account.

Power limitation: Ad hoc enabled mobile nodes are small and lightweight; therefore, they are often supplied with limited power resources, small batteries, to ensure portability. The security solution should take this restraint into account. Furthermore, this limitation causes vulnerability since a node powering-off can cause its break-down. Thereby, attackers may targets some nodes batteries to disconnect them, even to make network partition. This is called energy starvation attack or sleep deprivation torture attack.

Memory and computation power limitation: Ad hoc enabled mobile nodes have limited storage devices and weak computational capabilities.

3.1 Challenges for MANETs

Mobile ad hoc networks face challenges when compared to wireless networks due following reasons[9]:

1. The wireless networks are liable to attacks because of active eavesdropping to passive interfering.
2. Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
3. Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
4. Due to MANET's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words

   We need to cover up from both insider and outsider attacks in MANET, in which insider attacks are more difficult to deal with.
5. It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

3.2 Methods to Face the Challenges

Challenges in MANETs are: Routing protocols, Node Mobility, Detecting channel error, key distribution, and authentication. To face these challenges methods used are[7]:

a) Multi-factor authentication in MANET

It is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. This multi-factor authentication scheme extends the cryptographic link, binding an entity to a physical node device. This is achieved by using two distinct authentication factors; certified keys and certified node characteristics. But the major drawback is that, the underlying networkings environment on which they are applicable have been left unspecified. As a result, lack of specifications about the networking environments applicable to an authentication protocol for MANETs can mislead about the performance.

b) A Distributed Authentication Scheme and Trusted Computing in MANET

With the rapid development of MANET, the secure and practical authentication problem in it increasingly becomes outstanding. In distributed authentication scheme, a secret key distributed storage scheme based on CRT-VSS and trusted computing is proposed for MANET. Utilization of trusted computing technology is done to solve two existing cheating problems in secret sharing area before. Besides, efficiency performance of such schemes is not good enough due to the exponential arithmetic with Shamir's scheme.

c) Authentication and dynamic key management protocol based on certified tokens for MANETs

It contains no pre-key distribution and key storage for making protected data transmission in vulnerable wireless link. The proposed protocol does not require an on-line centralized authority in the active phase of the network. A hybrid cryptographic technique is used, which is a combination of RSA and elliptic curve cryptography (ECC) to achieve efficient mutual authentication and key agreement. Proposed protocol requires reasonable resources in terms of computation and communication overhead and provides higher security, which is suitable for value added applications, using MANET nodes.

d) Key distribution with entity authentication for efficient, scalable and secure group communication in MANET

The fact that, i) no central authorization entity is assumed at all times for all nodes which makes the task of network operations more difficult[10] and ii) indicates the need for distributed algorithms to provide the functions of centralized entities. KM ensures communication security among nodes and the capability of their cooperation as a secure group. It consists of key generation, user authentication and key distribution services.

e) Joint Authentication and Topology Control

The authentication schemes have significant impacts on throughput. Specifically, the effective throughput with upper layer authentication schemes and physical-layer schemes are analyzed related to channel conditions and relay selections for

CCs. A joint authentication and topology control (JATC) scheme is proposed to improve the throughput. JATC is formulated as a discrete stochastic optimization problem, which does not require prior perfect channel status but only channel estimate. Security has become the main concern and bottleneck for widely deployed wireless applications. Then, a joint authentication and topology control (JATC) scheme is proposed to adaptively tune the network configurations to optimize the effective throughput and the efficiency of authentication protocols for CC-MANETs. The objective of authentication is achieved by adjusting some controllable parameters that affect link status, such as transmission power, antenna direction, channel assignment, cooperative level, and transmission manners.

In general, distributed topology control schemes are desired to handle all the neighbor links, rather than a single link. As a result, use of another metric named aggregate throughput per node, this is nothing but the network throughput capacity per node.

4. COMPARATIVE STUDY

Different methods used in mobile ad hoc networks are compared in table as below.

Method	**Advantages**	**Disadvantages**
Preventing impersonation attacks in MANET with multi-factor authentication [1]	It drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information.	MFA approaches remain vulnerable to Phishing, man-in-the-browser and man-in-the-middle attack. They also Lack of specifications about the networking en--vironments.
Distributed Authenticatio n Scheme and Trusted Computing Secure Dis-tributed Authenticatio n scheme based on CRT-VSS and Trusted Computing in MANET[3]	distributed authentication scheme based on trusted computing eliminates the possibility of the malicious attack, e.g. DoS attack and fault attack, during the process of signature generation	The secure and practical authen-tication problem in it becomes Outstanding.
Authenticatio n and dynamic key manage-ment protocol based on certified tokens	As its function is generalized it is suitable for different types of routing protocols.	It contains no pre-key distribu-tions and key storage for making protected data transmission
Minimal Trusted Computing Base for MANET nodes[4]		
A trust system in MANET with secure key authentication mechanism Composite Trust-based Public Key Management in MANETs	this protocol performs normally even when a large percentage of the nodes in the network are malicious.	More vulnerable to malicious at-tacks from other related systems.

5. SUMMARY

For different topologies and requirements, different methods are used to tailor the mobile ad hoc networks. But these methods are not yet full proof as depending on requirement one has to change the design. Also dynamic nature of networks becomes the main point while applying different algorithms. If dynamic nature and authentication of users is taken care off then mobile ad hoc networks prove be the best ones to represent real life problems. Future work for MANETS is designing of good routing algorithm which handles the dynamic nature of /MANET is designed. If algorithm which mirrors vehicles going on road in accurate manner is designed it will be possible to develop vehicle to vehicle communication system. Such systems will prove beneficial in near future as everyday number of vehicle users are increasing and so the probability of accidents. Future Work is to design Mobile ad hoc networks which ensure secure message transfer in network.

6. ACKNOWLEDGMENTS

I am profoundly grateful to Prof. Ram Joshi for his expert guidance and continuous encouragement throughout to see that this review work rights its target since its commencement to its completion. His invaluable guidance supported me in completing this survey. At last I must express our sincere heartfelt gratitude to all staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

7. REFERENCES

[1] Quansheng Guan, Richard Yu, "Joint Topology Control and Authentication De- sign in Mobile Ad Hoc Networks With Cooperative Communications", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 6, JULY 2012.

[2] Na Ruan, Yoshiaki Hori, "DoS attack-tolerant TESLA-based broadcast authenti- cation protocol in Internet of Things", 2012 International Conference on Selected Topics in Mobile and Wireless Networking, pp 60 65, Apr. 2012.

[3] Qiwei Lu, Wenchao Huang, Xudong Gong, Xingfu Wang, Yan Xiong, and Fuyou Miao A Secure Distributed Authentication scheme based on CRT-VSS and Trusted Computing in MANET.

[4] Qiwei Lu; Yan Xiong; Wenchao Huang; Xudong Gong; Fuyou Miao, "A Dis- tributed ECC-DSS Authentication Scheme Based on CRT-VSS and Trusted Com- puting in MANET", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 656 665, 2012

[5] Maity, S.; Hansdah, R.C., "A Secure and Efficient Authentication Protocol (SEAP) for MANETs wIth Membership Revocation", 27th International Con- ference on Advanced Information Networking and Applications Workshops, pp363 370, 2012

[6] Pallavi D. Dudhe et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April-2014, pg. 671-676

[7] Int. J. Advanced Networking and Applications Volume: 6 Issue: 2 Pages: 2253-2261 (2014) ISSN : 0975-0290

[8] (IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Networks

[9] International Journal of Computational Engineering Research Vol, 03 Issue, 6

[10] Maria Striki, John S. Baras, Towards Integrating Key Distribution with Entity Authentication for Efficient, Scalable and Secure Group Communication in MANETs