A Comparative Study on Authentication Schemes for Mobile Networks

J. Santhosh
Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India

Sisha V A
M. Phil Scholar, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India.

Abstract – Authentication of mobile nodes are more challenging when the mobile networks are decentralized and with high dense. Due to the fast and frequent topological changes it is more convoluted task of authentication. Cryptographic keys are used to deploy the security for the decentralized wireless networks. It is very crucial to adopt for the dynamic and high mobility networks. Different techniques and authentication methods are proposed to tackle security issues in wireless networks. To develop a new successful method needs a complete review and problems of existing authentication and security methods in wireless mobile networks. This paper provides a comprehensive analysis and survey of those techniques with performance measures.

Index Terms – Wireless Mobile networks, authentication, security, key distribution, Trust management.

1. INTRODUCTION

Wireless Mobile Network technology is ultimately providing different types of services. Many researchers found different types of security threats [1] possible for a mobile network. The mobile network suffers from a set of possible attacks in various layers like black hole, wormhole and routing attacks etc. To secure the network from these attacks is the all-time target of several researchers. Although secure communication in a Mobile Network is often an essential system requirement, it is a challenging task due to unexpected mobility, lack of infrastructure, dynamic topology, and wireless nature of transmission. Among all the security services in mobile network, authentication is the most complex and important issue. Authentication provides the means to verify the identity of a node that participates to the monitoring tasks [2]. In order to conquer this, many authentication schemes, key generation and pre-distribution schemes have been proposed. Several key pre-distribution schemes are developed in which a large pool of key is chosen and keys are assigned to each node randomly by selecting from the large key pool. This paper surveys about the techniques and methods involved in the mobile network authentication and security issues. The security services of ad hoc networks are not altogether different than those of other network communication paradigms. Specifically, an effective security paradigm must ensure the following security primitives such as identity validation for mobile nodes, data confidentiality verification, access monitoring and controlling. However, the solutions to the concerns have been developed and widely deployed in the static infrastructure domain, which are often comprised of small resources. The security of the mobile nodes should satisfy a set of features as stated below.

Decentralized:

Like ad hoc networks themselves, attempts to secure themselves: they must establish security without *a priori* knowledge or reference to centralized, persistent entities. Instead, security paradigms must levy the cooperation of all trustworthy nodes in the network.

Proactive and Reactive:

Ad hoc networks are dynamic and infrastructure less. The trust calculation of nodes should support both proactive and reactive. The malicious behavior or attempt should be found quickly. Security paradigms must react to changes in network state and that must seek to detect compromises and vulnerabilities. The techniques should be reactive and proactive, not only protective.

Fault Tolerant:

The mobile networks topologies are unreliable and changes often. Nodes are likely to leave or be compromised without any cause. The communication requirements of security solutions should be designed with such faults in mind and they shouldn’t rely on message delivery or ordering.

Lightweight:

Solutions must minimize the amount of computation and communication required to ensure the security services to accommodate the limited energy and computational resources of mobile, ad hoc–enabled devices.

2. LITERATURE REVIEW

With the aim of providing complete authentication and security in mobile networks, many approaches were introduced. However, very few methods concentrated on the above security features. All features like reliability, scalability, trust worthy computation [3] with limited resource consumptions are not done together. The following literature review addresses the issues related to the research on the above mentioned scenarios. Various types of authentication schemes have been proposed in wireless network security, but as new threats and attack models are introduced, more need to be developed. The followings are the various aims of the authentication schemes [4].

1. Source authentication: This is the main goal of authentication techniques for the broadcast transmission. Validating the identity of the source from which the message originates is the most important property of any broadcast authentication protocol. Hence, it is required that each of the receiver(s) receiving a broadcasted message perform the source authentication.

2. Data integrity: It is also essential to maintain the integrity of the data contained in the message. Data integrity is maintained by making sure that the message content has not been modified or altered in the transmission, i.e. after being sent by the sender and before being received by the receiver(s).

3. Non-repudiation: It affirms that the source sending the message can never deny that it has sent the message.

For instance, digital signatures are the authentication certificates for the digital world similar to an individual’s signatures in non-digital world. Therefore, these authentication certificates contained in the messages are considered as legitimate proofs for the fact that the sender is the original author of the message. Hence, digital signatures ensure non-repudiation.

4. Immediate authentication: It is achieved if there is no delay between the reception of the message and its acceptance or rejection. Most of the MAC protocols with delayed key disclosure do not support this property. Hence, these protocols are not applicable in highly time critical systems unless other provisions are provided. Digital signatures, however, have no authentication delay and support immediate authentication property if they are not amortized.

5. Robustness to packet loss: The phrase robustness to packet loss is used with respect to authentication information loss. For instance, in MAC based protocols with delayed key disclosure, if the packet containing key is lost then the corresponding message cannot be authenticated. Hence, most of the TESLA-based schemes use one-way key chains. This way, if a key is lost, it can be recovered from future keys. However, digital signature schemes are robust to these types of losses as they do not require separate authentication packets.

6. Cryptographic method: Cryptographic schemes either use symmetric key MAC schemes or asymmetric key digital signature schemes. The digital signature schemes can either be one time schemes or public key based schemes. In the comparison table, this give the names of the specific symmetric or asymmetric schemes used in the protocols surveyed.

7. Support for multihop: It is the latest requirement for all recent and upcoming wireless networks. Precisely, it is important for broadcast authentication protocols to support multihop communication such that the number of false positives in multiple hops is as low as possible. The complete approach to providing multihop support in a broadcast authentication protocol is to authenticate each forwarded broadcast at every hop. There are additional costs for implementing these mechanisms which need to be traded off by compromising security using smart and hybrid techniques.

8. DoS attack resistance: Resistance to Denial-of-Service attacks is necessary for making sure that the broadcast authentication protocol performs its activities without interruption. This consider a protocol as DoS resistant if the protocol provides a countermeasure for one or more of the DoS attack, mainly flooding and jamming.

9. Loose time synchronization: It is a required property between the sender and receiver(s) for some protocols, such as MAC-based protocols and some of the digital signatures protocols. In MAC schemes, loose time synchronization aids the receiver(s) by making sure that at the time when a message is received, the corresponding key has not been released by the sender. This is called the security condition check.

10. Communication overhead: Most of the MAC based protocols have low communication cost while that of digital signature based protocols is influenced by the public key size. Resource constrained networks have a high requirement for protocols with low communication overhead. Most of the sensor networks and vehicular networks require low communication overhead.

11. Computation overhead: Inclusion of security procedures such as authentication increases computation overhead. In MAC-based protocols, computation is mainly done at the sender end while the receiver computation overhead is negligible. Therefore, this do account for the receiver computation in the comparisons. Comparatively in digital signatures, computation overhead is accountable both in signature generation and verification as given in the comparison table.

12. Buffering overhead: It influences the resources of the wireless communicating nodes. It can occur in two ways: either the buffering period is very long or the storage utilization is high. MAC-based protocols encounter the issue of having to buffer for a longer period if keys are lost or the system is designed for a longer key disclosure delay; hence, requiring long buffering periods at either the sender or the receiver(s). On the other hand, in digital signature schemes, buffering are only required with the signature amortization or similar schemes because digital signatures basically support immediate authentication with no need for buffering.

13. Scalability: This is considered distinctively in MAC and digital signatures. In MAC-based schemes, it is necessary to account for the number of senders and receivers that can be included in the authentication protocol. For instance, lTESLA schemes require only the base station to be the sole broadcast sender. On the other hand, digital signature schemes have no issues with the number of senders and receivers as each one constructs and verifies its signature independently. However, one-time signatures limit message authentications. Therefore, this will account for the scalability in digital signatures as the number of messages that can be sent by a sender.

2.1 KEY MANAGEMENT APPROACHES IN MOBILE NETWORKS

For node authentication in wireless mobile networks, key management is the popular technique. Key management is the set of techniques and procedures which support the establishment and maintenance of keying relationships between authorized nodes, and covers the following such as Node initialization; this starts the initialization process in the network. The second one is key setup, key generation and distribution follows to the second step. Updating and authentication key revocation is the final process. A keying relationship is the state wherein nodes share common data in cryptographic techniques. This data may include public or private key pairs, secret keys, initialization values, and non-secret parameters. The fundamental function of key management schemes is the establishment of keying material, which in turn can be subdivided into agreement on a key and transport of this key. Key management process allows two or more nodes to derive shared keying material as a function of information contributed by or associated with each of the protocol participants, such that no node can predetermine the resulting value. The key management can be achieved using either symmetrical or asymmetrical techniques. A hybrid key establishment approach makes use of both techniques in an attempt to exploit the advantages of each. The fundamental problem in Mobile Network security is to initialize secure communication between mobile nodes by setting up secret keys between communicating nodes. In general this is called key establishment. There are three types of key establishment techniques: the trusted-server approach, the self-enforcing approach, and the key pre-distribution approach.

Trusted Server Approach: The trusted server approach depends on a trusted server e.g., Kerberos. Since there is no trusted infrastructure in mobile networks, the trusted-server approach is fundamentally unsuited to them. Trust computations are recently used by several methods. However the decentralized dynamic dense mobile networks failed to perform the trust calculation from the neighbor node information.

Self-enforcing Approach: The self-enforcing approach depends on asymmetric cryptography using public keys. However, limited computation resources in mobile nodes make this approach less desirable. Public key algorithms such as Diffe-Hellman and RSA (William Stallings 2002) require high computation resources that the tiny mobiles cannot provide. But nowadays research is focused on to introduce public key schemes that are more suited for WMNs environment, which is discussed later in this thesis.

Key Pre-distribution Approach: The key pre-distribution approach, where key information is embedded in the mobile nodes before they are deployed seems a more appropriate solution for wireless mobile networks. While a simple solution is to store a secret master key in all the nodes and obtain a new pair wise key, the capture of one node will compromise the whole network. Storing the master key in tamper resistant mobile nodes increases the cost and energy consumption of the mobiles. Key pre-distribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position. Key pre-distribution schemes are developed by researchers for a better maintenance of key management in Mobile Networks. Basically a key pre-distribution approach has three phases, key distribution, shared key discovery and path-key establishment. During these phases, secret keys are generated, placed in mobile nodes and each mobile node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each approach), and communication between those two nodes takes place. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key pre-distribution approach used.

1.2 Key pre-distribution methods for mobile networks:

In paper [5], authors introduced hashed random preloaded subsets (HARPS), a highly scalable key pre-distribution (KPD) scheme employing only symmetric cryptographic primitives. This technique is ideally suited for resource constrained nodes that need to operate for extended periods without active involvement of a trusted authority (TA), as is usually the case for nodes forming ad hoc networks. It is a probabilistic key pre-distributed scheme, which is a generalization of two other probabilistic key pre-distribution. The first, random preloaded subsets (RPSs), is based on random intersection of keys preloaded in nodes. The second, proposed by Leighton and Micali (LM) is a scheme employing repeated applications of a cryptographic hash function. Authors investigated many desired properties of HARPS like scalability, computational and storage efficiency, flexibility in deployment modes, renewability, ease of extension to multicast scenarios, ability to cater for broadcast authentication, broadcast encryption, etc., to support its candidacy as an enabler for ad hoc network security.

In the paper [6], a probabilistic asymmetric key pre-distribution is proposed by the author, this improves basic Probabilistic asymmetric key pre-distribution (PAKP) scheme. The proposed algorithm can distinguish between different possible paths and choose that one which is the most reliable and trustful. The main advantage of this technique is it eliminates malicious nodes from dropping or modifying packets selfishly or maliciously. Subjective logic is used to model trust between nodes and also path conditions in this apepr. The model gathers cooperative observations from other nodes and provides sufficient information to choose the most robust and secure route. Incorporating this model leads to decreased traffic volume and improved security because the least number of trusty nodes are chosen as intermediate nodes. Besides, the enhanced model remains compatible with MANET's characteristics such as storage and computation limits and also the dynamic nature of topology. This reduces intermediate decryption-encryption steps. This also reduces the probability of malicious nodes to be chosen as a cooperating node. The most important result could be concluded from this paper is that with appropriate subjective logic based models one can improve cooperative protocols in heterogeneous MANETs. The trust model in heterogeneous MANETs implies how much evidence from a node is reliable while remaining models guide node's activities just like path selection in the context.

In the paper [7], authors proposed a novel solution based on DSSS and spread-code pre-distribution to achieve jamming resilient neighbor discovery in MANETs (JR-SND). It can enable two neighboring nodes to successfully discover each other with overwhelming probability despite omnipresent jammers. The efficacy and efficiency of the schemes are confirmed by detailed theoretical analysis and simulation results. However, this is only suitable for moderated density mobile network.

In the paper [8], authors have developed a key generation protocol for the IBC. In this IBC is a subclass that does not restrict the key cryptography. IBC is tending to remove the need for certification authority (CA) and public key certificates (PKCs). In this IBC for a user that is given is used as user's public key and private key which is depend upon the individuality of the user. In this IBC scheme the user is unrestricted with the designed function identity when the user's private key is being used by the trusted authority. In this IBC scheme the users are not restricted easily and they are easily designed function with the identity of the private key that is PKG. When comparing with the traditional PKI(public key infrastructure) the IBC is required in order to transmit and store the large volume of certificates and public key hence MANET is used.

3. CONCLUSION

In this paper, we investigated the authentication techniques for wireless mobile networks. We first presented the challenges of authentication schemes in the mobile networks. Then, we presented an analysis of existing authentication approaches in the pre-key distribution techniques: the organization of the network, the purpose of the authentication tasks, how authentication data is collected and which algorithm is used. We then surveyed all existing authentication approaches. This survey highlighted the richness and diversity of the recent solutions for the authentication. In fact, existing solutions are different and rely on different paradigms and protocols. Some of the approaches are part of more complex management solutions which are applicable only in specific wireless sensor networks. This is very common because the authentication of wireless sensor network is possible due to its centralized authentication server and limited boundary. It is more simple and fast. Although, they have several merits, it is quite good to establish a new technique for decentralized authentication scheme for mobile networks. The highlight of this survey is that authentication approaches for mobile networks are too ambitious and tend to apply what is commonly used in infrastructure-based networks.

REFERENCES

[1] Pathan, Al-Sakib Khan, ed. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[2] Zhou, Lidong, and Zygmunt J. Haas. "Securing ad hoc networks." *IEEE network* 13.6 (1999): 24-30.

[3] Govindan, Kannan, and Prasant Mohapatra. "Trust computations and trust dynamics in mobile adhoc networks: A survey." *IEEE Communications Surveys & Tutorials* 14.2 (2012): 279-298.

[4] Papadimitratos, Panos, and Zygmunt J. Haas. "Secure routing for mobile ad hoc networks." *the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002*. 2002.

[5] Ramkumar, Mahalingam, and Nasir Memon. "An efficient key pre-distribution scheme for ad hoc network security." *IEEE Journal on Selected Areas in Communications* 23.3 (2005): 611-621.

[6] Gope, Prosanta. "Enhanced secure mutual authentication and key agreement scheme with user anonymity in ubiquitous global mobility networks." *Journal of Information Security and Applications* 35 (2017): 160-167.

[7] Zhang, Rui, Jingchao Sun, Yanchao Zhang, and Xiaoxia Huang. "Jamming-resilient secure neighbor discovery in mobile ad hoc networks." *IEEE Transactions on Wireless Communications* 14, no. 10 (2015): 5588-5601.

[8] Narayana, V. Lakshman, and C. R. Bharathi. "IDENTITY BASED CRYPTOGRAPHY FOR MOBILE AD HOC NETWORKS." *Journal of Theoretical and Applied Information Technology* 95.5 (2017): 1173.