A Survey on Present Mobile Ad-Hoc Networks (MANET) Security

Chetna Vaidya[1]* Dr. M. K. Bisht[2]

[1] Research Scholar

[2] Pacific University, Rajasthan, India

Abstract – The wireless mobile nodes are capable to build spontaneously temporary wireless network in absence of infrastructure like AP, Router etc. and they act as a wireless router. Due to this, wireless mobile nodes are capable for forwarding messages to other nodes. MANET (Mobile Adhoc Network) is a one of the wireless network and forms a temporary connection across the mobile nodes without central infrastructure to exchange the information. Due to the characteristics of MANET, it is vulnerable to active and passive attacks from internal and external attacker. This will lead to various security challenges. There is a requirement to secure the MANET from threats and vulnerability. Many security mechanisms are established to secure and protect the MANET. This article is intended to provide contemporary MANET security with perspective of routing protocol security and data security with key management, and monitoring the MANET during routing and/or data transmission using IDS (Intrusion Detection System). This article presents the various attacks face by MANET and its security goals. The article explored various security solutions for routing protocols, data security using cryptography as a first line of defence, key management for securing communication. It also explored various IDS schemes as a second line of defence in MANET.

Keyword- Cryptography, Data Security, Attack, IDS, Routing Protocol, Secret Sharing

- X -

INTRODUCTION

Wireless Adhoc Network is a temporary connection across the nodes without central infrastructure for exchanging the information. Both Bluetooth (IEEE 802.15.1) and IEEE 802.11 are the main wireless ad hoc network technology. MANET is a self-organized and less infrastructure temporary wireless network where the contents are transferred from node to node. In this environment, all nodes are equally works as a router. The MANET's characteristics are wireless link as a shared medium, dynamic topology, node mobility, limited energy, limited resources, distributed operations, fewer infrastructures, self-organized; all nodes are not trusted, multipath route etc. MANET has unique challenges due to its characteristics. Hence, MANET is vulnerable toward a great variety of attacks due to its challenges. However, MANET is flexible, scalable, relatively cheap and easily deployable at any place and time because of its characteristics. On the other side, the MANET is vulnerable to availability, integrity, privacy, indeed, eavesdropping and interception. It is also vulnerable to node suppression, node replication and node impersonation due to self-organized topology. Secure routing; security of content transfer, quality of service (QoS) and service discovery are the main security goals in Adhoc networking. MANET can be used in tactical networks like military communication and operations, emergency services like disaster recovery and rescue operation, commercial sector like networks of visitors at airports and PAN (Personal Area Network), enterprise networking like networks at construction sites, education network like virtual classrooms, entertainment network like multi user games, sensor network like animal movement, context aware services and coverage extension like linking up with the Internet, intranets etc.

REVIEW OF LITERATURE:

Mobile Ad hoc Networks (MANETs) are infrastructure-less networks comprising mobile nodes and are vulnerable to attacks for lack of any specific boundary and random entry of nodes in the network. Authentication is the hallmark of security and failure to achieving this so far is a stumbling block in the way of securing MANET. At small scale the authentication can be managed by the nodes through handshaking (Lin and Hovy, 1997), but at larger scale it becomes complex and demands the involvement of TTP (Isa, et. al., 2008). Some of the schemes are either based on self-organization in MANETs without TTP (Goyal, 2007) where the identity is resolved by nodes themselves and some are based on absolute TTP (Zhao and Li, 2009), while a hybrid form of these schemes can also be used (Isa, et. al., 2008). This research work is based on the optimization of a scheme known as Tseng model (Isa, et. al., 2008) that gets the nodes authenticated in MANET by the use of 4th generation (4G) technology (Lin, 2010) and (Zhang and Li, 2009), a future technology that supports in communicating different platforms in a transparent manner. The Tseng model allows the authentication and distribution of certificates to nodes through the support of 4G technologies. The Tseng model did not take into account the CRL status of servers. The Tseng model shows further overheads if this feature is embedded in the scheme, since, the nodes need to check frequently the server's CRL status for authenticating a node and place external messages outside MANET. If a server finds its ID in the CA's CRL directory any time it renders all the certificates of nodes invalid in the MANET. The nodes ask their servers to find the CRL status of a corresponding node's server. The communicating nodes can be from same and different CA domains. In the worst case if nodes need to establish sessions with the nodes from different servers each time, the overhead grows even more. The Tseng model, not fulfilling the requirement of CRL for the nodes to be known before authentication, can be regarded as less secure and costly for overheads when the nodes from different servers try to communicate and verify from servers with the added feature of security.

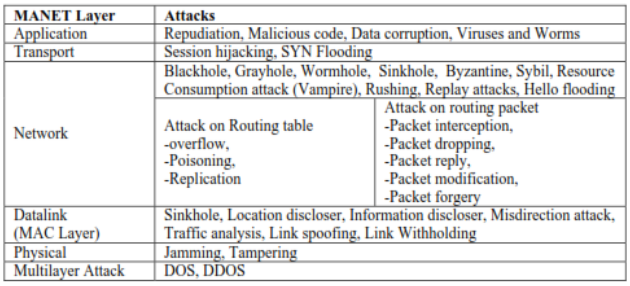
NETWORK TRAINING

It is vital of no calculation right now accessible which can ensure worldwide ideal answer for general nonlinear streamlining issues, for example, those in neural network preparing. Indeed, all calculations in nonlinear advancement unavoidably experience the ill effects of the neighborhood optima issues and the most we can do is to utilize the accessible streamlining technique which can give the "best" nearby optima if the genuine worldwide arrangement isn't accessible. It is likewise imperative to bring up that the steepest plummet strategy utilized in the essential back proliferation endures the issues of moderate intermingling, wastefulness, and absence of power. Moreover, it inclines to be extremely delicate to the decision of the learning rate. Littler learning rates will in general moderate the learning procedure while bigger learning rates may cause organizes swaying in the load space. Basic adjustments to the fundamental back proliferation incorporate including the load refreshing recipe (2) an extra energy parameter relative to weight modification the to controller the swaying in weightiness modifications and (3) a load rot term that punishes the excessively composite Net-system with vast loads. Network preparation for order and expectation issues is completed by resources of administered learning in which known yields and their related information sources are both exhibited to the network. Neural network preparing suggests to the procedure in which these loads are resolved, and subsequently is the method the network studies.

MANET SECURITY

The main security goals/requirements are availability, integrity, confidentiality, authentication and nonrepudiation. As oppose to this, the main goal of attacker is to violate the security goal through resource consumption, routing disruption and packet leashes. Attacks in MANET are classified based on the status of attacker, behaviour of attack, and the purpose of the attack. The status of the attacker could be either; internal (insider) in case of malicious node present within the network or external (outsider) in case the malicious nodes do not belong to the network. The behavior of attacks could be either active attack like prevention of message flow between the nodes or passive attack like unauthorized listening to the network traffic for traffic analysis or accumulating data from it. Further, active attacks can be classified into four categories: dropping attacks, modification attacks, fabrication attacks and timing attacks. Based upon the purpose of attack, attacks can be categorized into three categories (Lin and Hovy, 2002): the purpose of illegal/invalid access like impersonation and masquerade, purpose of stealing like eavesdropping, snooping and interception, and purpose of targeting content or resource to make an active operation like a reply, Denial of Service (DOS) and packet drop (black hole, gray hole). MANET is comprised of layers such as physical layer, data link layer, network layer, transport layer and application layer. Table 1 shows the various possible attacks at different layers of MANET.

TABLE I Attacks at different layers of MANET



MANET Layer	Attacks	
Application	Repudiation, Malicious code, Data corruption, Viruses and Worms	
Transport	Session hijacking, SYN Flooding	
Network	Blackhole, Grayhole, Wormhole, Sinkhole, Byzantine, Sybil, Resource Consumption attack (Vampire), Rushing, Replay attacks, Hello flooding	
	Attack on Routing table -overflow, -Poisoning, -Replication	Attack on routing packet -Packet interception, -Packet dropping, -Packet reply, -Packet modification, -Packet forgery
Datalink (MAC Layer)	Sinkhole, Location discloser, Information discloser, Misdirection attack, Traffic analysis, Link spoofing, Link Withholding	
Physical	Jamming, Tampering	
Multilayer Attack	DOS, DDOS	

The MANET can be secured using cryptography, secure routing mechanisms and IDS or may use the combination of these approaches. Cryptographic method and IDS can protect the MANET before information (control) and/or after information (data) forwarded while secure routing mechanism can protect the control (routing) information and discover dynamically reliable routes (Lin and Hovy, 1997) which can be either proactive or reactive (Barzilay and Elhadad, 1997).

SECURE MANET ROUTING PROTOCOLS

Position based, proactive, reactive, topology based and hybrid are the strategies of MANET routing protocol. The routing protocols are classified based on acquired routing information such as proactive information or reactive information, fundamental differences among nodes such as uniform (every node plays equal role or equal important is given to all node: flat) or non-uniform (cluster/zone: hierarchical), path construction metric such as stable link or hop count (major protocol uses (Marcu, 1998)), topology based routing information in which the routing protocol gives complete list of intermediate nodes, destination based in which the routing protocol gives list of only next hop and location based in which mobile nodes access geographical information. To secure the routing protocol, majority of protocols use the cryptography. The node who wishes to participate in the routing process must trusted nodes. Authentication based technique can be used to discover the trusted nodes. These trusted elements work according to defined rules of protocol. Authentication can be implemented using symmetric, public key or digital signature. Routing information is significantly control information rather than the data. Hence, it cannot be encrypted (mutable filed) which is still remain useful. Secure routing protocol provides the reliable and accurate path in the presence of untrusted network or malicious attackers (Carbonell and Goldstein, 1998). ALARM (Anonymous Location-Aided Routing in MANET) (Lin, 2010) is an anonymous secure location based routing protocol. ALARM finds node's current location by flooding the LAM (Location Announcement Message) throughout the MANET. It then constructs topology utilizing the node's location. It is based on advanced cryptographic group signatures, a public key signature which provides both security and privacy. ALARM provides authentication, integrity, anonymity, and un-traceability. It also provides protection from passive and active attacks as well from internal and external attacks.

MANET DATA SECURITY

We have discussed the various proposed approaches to secure the routing protocol. But MANET cannot be secured 100% by using only secure routing protocol. Hence, MANET requires first level of defense i.e. cryptography in MANET for securing the data. However, once cryptography involved in MANET, the extra overhead may affect the performance of MANET. Cryptography plays a vital role for MANET security. IBC (Identity Based Cryptography) is used for key distribution without Key Distribution Center (KDC) or Trusted Third Party (TTP) or Certificate Authority (CA). It is effective in MANET for key management, data security and routing protocol security. Authors demonstrated and compared major strengths and weaknesses of various IBC based schemes. IBC requires a Key Generation Center (KGC) to distribute the private-public pair keys to all the nodes before starting the cryptographic operation. Due to this dependency on KGS, IBC hampers the true nature of ad-hoc networks. Identity-based RSA (Id-RSA) model is a lightweight authentication and encryption scheme for MANET. Id-RSA model performs fast cryptography operations that enhance network performance. Authors compared this model with RSA Threshold Cryptography (RSA-TC) and ECC based Threshold Cryptography (ECC-TC) with respect to cryptography operation execution time and overhead caused due to security messages. They proved that RSA-TC and ECC-TC increase delay and overhead as compared to Id-RSA. In authors improved Id-RSA by removing certificate authentication scheme which in turn requires less computational cost than Id-RSA.

A novel Device to Device (D2D) authentication mechanism is proposed for security. This mechanism uses secure initial key establishment using Cipher text Policy Attribute Based Encryption (CP-ABE). Communicating devices mutually authenticate each other and derive the link key. This scheme provides protection against Man in the Middle (MIM) and replay attacks. A hash chain based public key encryption algorithm has been introduced for MANET. Authors used Montgomery algorithm with hash chain for public key distribution in the scheme. Montgomery is an algorithm that reduces division in modular multiplication compared to RSA. In authors used a credit based cooperation mechanism with hash chains for both routing and data forwarding messages. With this scheme, computational overhead of the node is reduced and security against malicious nodes is provided. In first transaction, only source node uses the digital signature. For further transactions, scheme uses only hash function instead of a digital signature for source node as well for all other intermediate nodes.

SECURITY ENHANCEMENT IN MANET

A lot of work has been done on security problems regarding MANETS so far. We now take a brief overview of some of the related previous papers as following. In threshold cryptographic scheme (Luhn, 1958), the authority of CA is distributed among many t+1 network nodes, called servers, to minimize the chance of a single CA being compromised. All the nodes' certificates are divided into n shares and distributed to server nodes before network formation. If a node requires other node's public key, it requests to server nodes which generate their partial signatures individually and send to combine to form a signature and present to the asking node. In MANET it is a cumbersome process that may cost more than a MANET's formation objective. A similar scheme (Lin and Hovy, 2002) is an improvement over (Luhn, 1958) on the basis of availability. Here, the CA is a fully distributed and any t+1 number of nodes in MANET could behave as server nodes for issuance and verification of public keys for the nodes. Despite the advantage of availability, the scheme loses on the side of robustness with the higher values of t. The selection of t should be trade-off between both of the parameters. In KAMAN (Barzilay and Elhadad, 1997), multiple Kerberos servers are responsible for distributed authentication in MANET. The servers are boot-strapped with keys shared with the client nodes. The users rely upon servers for acquiring tickets after authentication to communicate with other users which is a bottleneck for its implementation in MANETs and the servers are not trusted as there is no TTP involved initially. In self-organized MANETS (Goyal, 2007), the nodes rely on themselves for all routing, authentication and mobility management. The nodes issue certificates to their trustees for bringing them into MANET which are verified on the basis of repositories maintained by the nodes. Though, the scheme is self-organized but has the overheads of maintaining repositories which consumes the memory and bandwidth. Secondly, the originator blindly trusts any other node for making a new entry in the MANET. A scheme (Isa, et. al., 2008) based on PKI implementation, resolves identity of nodes in MANET with the help of 4G services. The server distributes certificates to nodes through a special node using 4G services. The scheme successfully embeds TTP with MANET and getting nodes authenticated. However, it shows external message overheads when nodes from different servers communicate and verify the server's CRL status frequently. The scheme can be further optimized by reducing the overheads. One more scheme (Zhao and Li, 2009) is based on certificate distribution to nodes before network formation by a trusted third party. The drawback remains with the condition of certificate issuance by TTP before network formation to all the nodes in MANET.

CONCLUSION

As MANET is a wireless Ad-hoc network, it has its own characteristics and features. It is vulnerable to active and passive attacks from internal and external attackers due to its characteristic and features. Single approach is not sufficient to secure MANET. Some security mechanisms can be used to prevent from malicious activity during path discovery process in MANET. To secure the data being transmitted, cryptography may integrate as a first level of defense. The IDS is used to monitor the network as a second line of defense. These solutions are application specific. Cryptographic method and IDS can protect the MANET before forwarded message (control) and/or after forwarded message (data). While secure routing mechanism can protect the control (routing) information and discover dynamically reliable routes. Besides using cryptography as first line of defense, some other security mechanisms like game theory, fuzzy, trust etc. can also be used during route discovery phase and data transmission. Performance of the network may goes down with the inclusion of security mechanisms that is negotiated as a tradeoff for supporting the need of security. There are more and more new applications in the commercial sector that are using MANET recently. Therefore, the success of this technology will largely depend on security of new applications and programs to be developed.

REFERENCES:

1. D. Isa, L. H. Lee, V. P. Kallimani, and R. Rajkumar (2008). “Text document preprocessing with the bayes formula for classification using the support vector machine,” IEEE Transactions on Applied Computational Intelligence and Soft Computing 9 Knowledge and Data Engineering, vol. 20, no. 9, pp. 1264–1272.

2. R. D. Goyal (2007). “Knowledge based neural network for text classification,” in Proceedings of the IEEE International Conference on Granular Computing (GrC ’07), pp. 542–547, November 2007.

3. H. P. Luhn (1958). “The automatic creation of literature abstracts,” IBM Journal of Research and Development, vol. 2, pp. 159–165.

4. H. P. Edmundson (1969). “New methods in automatic extracting,” Journal of the ACM, vol. 16, no. 2, pp. 264–285.

5. C.Y. Lin and E. H. Hovy (2002). “Manual and automatic evaluation of summaries,” in Proceedings of the ACL-02 Workshop on Automatic Summarization, vol. 4, pp. 45–51.

6. C.Y. Lin and E. H. Hovy (1997). “Identifying topics by position,” in Proceedings of the 5h Conference on Applied Natural Language Processing, pp. 283–290.

7. R. Barzilay and M. Elhadad (1997). in Proceedings of the ACL Workshop on Intelligent Scalable Text Summarization, Using lexical chains for text summarization, Ed., pp. 10–17.

8. D. Marcu (1998). “Improving summarization through rhetorical parsing tuning,” in Proceedings of the 6th Workshop on Very Large Corpora, pp. 206–215.

9. J. Carbonell and J. Goldstein (1998). “The use of MMR, diversity based reranking for reordering documents and producing summaries,” in Proceedings of the ACM 21st International Conference on Research and Development in Information Retrieval, pp. 335– 336.

10. J. Lin, N. Madnani, and B. J. Dorr (2010). "Putting the user in the loop: interactive maximal marginal relevance for query-focused summarization," in Proceedings of the Annual Conference of the North American Chapter of the Association for Computational Linguistics (HLT'10), pp. 305–308, June 2010.

11. P.-Y. Zhang and C. H. Li (2009). "Automatic text summarization based on sentences clustering and extraction," In Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT '09), pp. 167–170, August 2009.

12. L. Zhao and C. Li (2009). "Ontology based opinion mining for movie reviews," in Proceedings of the 3rd International Conference on Knowledge Science, Engineering and Management, pp. 204–214.

Corresponding Author

Chetna Vaidya*

Research Scholar