A Review: Various Security Mechanisms used in MANET

Vaishali V. Sarbhukan#1, Dr. Lata Ragha#2
#Department of Information Technology,Terna Engineering College, Nerul, Navi Mumbai
#2 Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi ,Navi Mumbai

Abstract-*In recent years, mobile ad hoc networks (MANETs) have become a popular research subject due to their self-configuration and self-maintenance capabilities. Wireless nodes can establish a dynamic network without the need of a fixed infrastructure. This type of network is very useful in tactical operations where there is no communication infrastructure.A significant part of the research work has focused on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. Unfortunately, the open medium, distributed nature and dynamic topology of MANET make it vulnerable to various types of attacks like black hole attack, grey hole attack, sybil attack, packet dropping attack and sleep deprivation attack etc. In MANET nodes are free to move arbitrarily with different speeds therefore network topology may change randomly and at unpredictable time. Therefore, security is main obstacle in tactical MANETs .In this paper detailed review is given on various mechanisms used for providing security in MANET.*

Keywords –*Cryptography, Mobile ad hoc Network, Payment, Reputation, Security, Trust*

I. Introduction

The concept of mobile wireless devices working together was proposed in the 1990s, since when a significant amount of research has been conducted on mobile ad hoc networks (MANETs) [1][2][3]. The IETF established the Mobile Ad hoc Networks Working Group in 1997, with the aim of standardizing routing protocols for MANETs. They developed two standard track routing protocol specifications, namely the reactive and proactive MANET protocols. Another IETF working group, called Ad Hoc Networks Auto configuration (autoconf), had as its main aim considering the issues in the addressing model for ad hoc networks. MANETs use IEEE 802.11 architecture components as described in [4]. The Basic Service Set (BSS) defines an architecture [5] in which all stations can communicate between themselves using IEEE 802.11 wireless LAN technology. A BSS consists of an access point (AP) and all the stations associated with it. Figure 1 shows the alternative ad hoc network architecture using the IEEE 802.11 independent basic service set (IBSS). MANET is of different types like VANET (Vehicular Adhoc Network), SPANS (Smart Phone Adhoc Networks) and iMANET (internet based Mobile Adhoc Network).

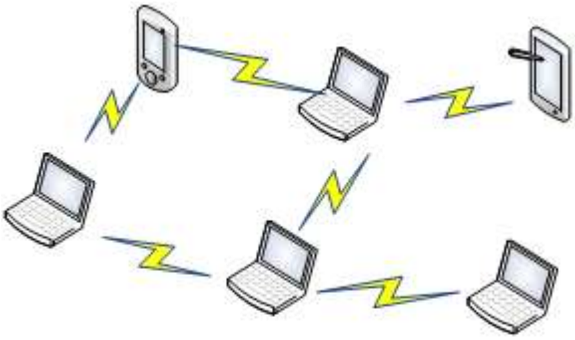

Fig. 1 Ad hoc architecture using IEEE 802.11 IBSS [5]

MANETs have wide applications in various fields. With recent advances in wireless technologies and mobile devices, mobile ad hoc networks (MANETs) have become popular as a key communication technology in military tactical environments such as the establishment of communication networks used to coordinate military deployment among the soldiers, vehicles, and operational command centers [6]. MANETS have been used in a military context to ensure the timely flow of information and command in battle, contributing to the success of a mission.There are many risks in military environments that need to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium,nomadic and distributed nature, and lack of centralized infrastructure of security protection. MANETs are also ideal for establishing communication networks and providing rescue services following natural disasters such as earthquakes or floods. Another major application of MANETs is on-the-fly collaborative computing outside an office environment, for example during fieldwork, in a team project offsite, or during an offsite meeting. MANETs can be used in communication dispatch systems for taxis in a town. In this paper survey is done on security approaches used in MANET on different basis.

II. Issues in MANET

2.1 Challenges in MANET Protocols

- Managing trust in a distributed Mobile Ad Hoc Network (MANET) is challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and reconfigurability.
- Security protocol designers for MANETs face technical challenges due to severe resource constraints in bandwidth, memory size, battery life, computational power, and unique wireless characteristics such as openness to eavesdropping, lack of specific ingress and exit points, high security threats, vulnerability, unreliable communication, and rapid changes in topologies or memberships because of user mobility or node failure.
- Designing security protocols for military MANETs requires additional caution, since battlefield communication networks must cope with hostile environments, node heterogeneity, often stringent performance constraints, node subversion, high tempo operations leading to rapid changes in network topology and service requirements, and dynamically formed communities of interest wherein participants may not have predefined trust relationships. To cope with these dynamics, networks must be able to reconfigure seamlessly, via low-complexity distributed network management schemes.

2.2. Issues with Mobile Ad Hoc Network Routing

Asymmetric joins: Most of the wired systems depend on the symmetric connections which are constantly fixed. Be that as it may, this isn't a case with ad hoc systems as the hubs are versatile and continually changing their situation inside system. For instance think about a MANET (Mobile Ad-hoc Network) where hub B sends a flag to hub A however this does not enlighten anything concerning the nature of the association in the turn around heading [7].

Routing Overhead: Routing in ad-hoc networks has been a testing assignment [8]as far back as the remote systems appeared. The significant purpose behind this is the consistent change in organize topology in light of high level of hub versatility. Along these lines, some stale courses are created in the routing table which prompts superfluous routing overhead.

Interference: This is the real issue with ad-hoc networks as connections go back and forth relying upon the transmission qualities, one transmission may meddle with another and hub may catch transmissions of different hubs and can degenerate the aggregate transmission.

Dynamic Topology: This is likewise the real issue with ad-hoc networks since the topology isn't consistent. The mobile hub may move or medium attributes may change. In ad-hoc networks, routing tables should by one means or another reflect these adjustments in topology and routing calculations must be adjusted. For instance in a fixed arrange routing table refreshing happens for each 30 sec[7] . This refreshing recurrence may be low for ad-hoc networks.

III. Literature Survey

There are mainly two approaches that can provide security in MANETs: prevention-based [9][10][11[12] approaches and detection based approaches. Prevention-based approaches are mainly based on cryptography and detection based approaches based on trust threshold.Example of Prevention-based approaches is cryptography based. Detection based approaches are further classified as reputation based , payment based, trust based. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed. Furthermore, although prevention-based approaches can prevent misbehaviour, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. From the experience in the design of security in wired networks, multilevel security mechanisms are needed. Therefore detection-based approaches are more preferred than preventionbased schemes.We will see all methods in detail.

3.1 Cryptography based Schemes

In [9]C. Adjih et al presented security architecture using OLSR routing protocol .Here main principles of the architecture are:

• For authenticated nodes: trust but verify. By default, the behavior of authenticated nodes is assumed correct. However it is assumed that one participant may start to act adversarily ,thus the policy is to perform ongoing checks.

• For unauthenticated nodes: protection. The aim is to prevent them to disrupt the network. In Authentication architecture[9], asymmetric (public key) cryptology is used. This is a requirement for the policy "trust but verify", since with respect to authenticated nodes, a necessary complement of "verification" is the step the traceability and accountability: when a trusted node misbehaves, being able to identify it among other nodes, is a necessity and a deterrent.

With traditional asymmetric cryptology, an issue is that public keys need to be distributed, hence a PKI infrastructure is needed. Some efficient proposals and implementations already exist for OLSR, such as [13], where a distributed certificate authority is introduced in the network: threshold cryptography is used so that a node in the network only need to connect the closest k authorities (and allowing also server redundancy).[9] presented preventing attacks like from authenticated nodes generation of incorrect control messages , not forwarding data packets, not forwarding control messages and attacks like wormhole attack, replay attacks and preventing packet transmission from unauthenticated nodes.

In [10] Y. Zhang presented IKM, an ID-based key management scheme as a novel combination of ID-based and threshold cryptography. IKM is a certificateless solution in that public keys of mobile nodes are directly derivable from their known IDs plus some common information. It thus eliminates the need for certificate-based authenticated public-key distribution indispensable in conventional public-key management schemes. IKM features a novel construction method of ID-based public/private keys, which not only ensures high-level tolerance to node compromise, but also enables efficient network-wide key update via a single broadcast message.

In [11] Y. Fang proposed schemes which rely on the ID-PKC, It is a perfect fit for WANETs, specifically for MANETs and WSNs.Although ID-PKC cannot completely replace conventional certificate-based PKC under all circumstances, it does provide more efficient, lightweight, and flexible solutions in many application scenarios such as resource constrained WANETs.In traditional public key cryptosystems, a user's public key is a string not related to his/her identity; thus, there is a need to provide an assurance (or binding) about the relationship between a public key and the identity of the holder of the corresponding private key. This assurance is delivered in the form of a certificate in the traditional

PKI. The PKI has to deal with the issues associated with certificate management, including revocation, storage, and distribution, and the computational costs of certificate verification, which often rely on reliable trustworthy infrastructure (certificate agency, CA). These issues are particularly acute in low-power and low bandwidth situations (e.g., in WANETs), where the need to transmit and check certificates has been identified as a significant limitation.

3.2 Reputation based Schemes

Reputation-based schemes [14] attempt to identify the malicious nodes that drop packets with a rate more than a pre-definedthreshold in order to avoid them in routing. When a node A sends a packet to the next node in the route B to relay to C, A has to overhear the channel to check whether B forwards the packet. If A does not overhear the packet transmission, it assumes that B has dropped the packet. Each node measures the frequency by which the other nodes drop packets in terms of reputation values. A increases the reputation value of B when it observes a packet transmission; otherwise,it decreases the reputation value of B. Once the reputation value degrades to a threshold, A identifies B as malicious.Reputation-based schemes suffer from false accusations where some honest nodes are falsely identified as malicious. This is because the nodes that drop packets temporarily, e.g., due to congestion, may be falsely identified as malicious by its neighbors. In order to reduce the false accusations, the schemes should use tolerant thresholds to guarantee that a node's packet dropping rate can only reach the threshold if the node is malicious. However, this increases the missed detections where some malicious nodes are not identified. Moreover, tolerant threshold enables the nodes with high packet dropping rate to participate in routes, and enables the malicious nodes to circumvent the scheme by dropping packets at a rate lower than the scheme's threshold. When a node's reputation value is above the threshold, it does not have incentive to relay packets because it does not bring more utility. Reputation-based schemes may identify the black-hole attackers that drop all the packets they are supposed to relay. However, they are less effective in detecting the gray-hole attackers that drop a portion of the packets. There is an unavoidable tradeoff between missed detections and false accusations. This is because determining an optimal threshold that can precisely differentiate between the honest and the malicious nodes is a challenge, especially in HMWNs. Using a threshold to determine the trustworthiness of a node is not effective in HMWNs because the nodes' packet-dropping rates vary greatly. Therefore, these schemes cannot guarantee route stability or reliability in HMWNs.

3.3. Payment Schemes

M. Mahmoud et.al [15] uses the payment system as a communication protocol that can transfer messages from the source node to the destination with limited use of the public key cryptography operations. Public key cryptography is used for only one packet and the efficient hashing operations are used in next packets.

In [16], payment is used to thwart the rational packet-dropping attacks, where the attackers drop packets because they do not benefit from relaying packets. A reputation system is also used to identify the irrational packet-dropping attackers once their packet-dropping rates exceed a threshold. The payment based methods [15] [16] work on efficient data transmission, however the trustworthiness of nodes to deliver the security as well as reliability for data transmission especially in high mobility networks. The proposed approach works not only works on stable and reliable route selection, but also secure data transmission. Payment Schemes Payment (or incentive) schemes use credits (or micropayment) to encourage the nodes to relay others' packets [17][18]. Since relaying packets consumes energy and other resources, packet relaying is treated as a service which can be charged. The nodes earn credits for relaying others' packets and spend them to get their packets delivered.

In Sprite [17], for each message, the source node signs the identities of the nodes in the route and the message. Each intermediate node verifies the signature and submits a signed receipt to TP to claim the payment. However, the receipts overwhelm the network because one receipt is composed for each message. To reduce the receipts' number, PIS [18] generates a fixed size receipt per route regardless of the number of messages.

3.4.Trust based Schemes

Theodorakopoulos et al [19] studies the problem of evaluating the trust level as a generalization of the shortest path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. The main goal is to enable the nodes to indirectly build trust relationships using exclusively monitored information.

Velloso et al [20] introduced human-based model which builds a trust relationship between nodes in ad hoc network. Without the need for global trust knowledge, they have presented a protocol that scales efficiently for large networks.

Lindsay et al [21] designed information theoretic model to quantitatively measure trust and model trust propagation in wireless networks. Trust is a measure of uncertainty with its value represented by entropy. The evidence collected for malicious and benign behaviors are probabilistically mapped by following a modified Bayesian approach.

Recently Shuaishuai Tan et.al [22] proposed the fuzzy logic based routing method to formulate imprecise empirical knowledge, which is used to evaluate path trust value. Along with the fuzzy logic, they adopted the graph theory to build the new trust system to compute the mobile nodes trust value. The filtering method designed to defend against the increasing attackers. The fuzzy rules mainly based on PDR rate of node. However using the fuzzy rules not solves the problem of reliable communication and stable routes in network.

Stylianos Kraounakis et al [23] proposed generalized computational model for trust establishment based on a reputation mechanism. The trust is computed by using the parameters such as experiences of service requestors (source nodes) and information disseminated from witness requestors (intermediate nodes) in the system on the basis of their past experiences with service providers. The reputation based approach delivers the efficient path for data transmission, but reliability and data security problems not solved by such methods. The trust values are computed by third party and hence may leads to the incorrect computation of trust values intentionally for security threat in network, thus the trust based methods are not always reliable method.

To solve this problem, Zhexiong Wei et.al [24] reported trust management approach using the uncertain reasoning. The attempt made to improve the MANET security using the existing trust based methods. The interpretation of node trust performed and recognizes the uncertainty in trust evaluation. Using such interpretation, the trust management model designed improves the MANET security. However, the excessive routing loads imposed by uncertain reasoning, also not solve the reliable path and secure data transmission problems.

IV. Conclusion

In this paper different security mechanisms used in MANET are reviewed. Major categories are prevention based approaches and detection based approaches. Every method is trying to remove loopholes of existing systems.They are categorized on basis of cryptography,reputation,trust, payment or combination of two methods like hybrid. Due to limitations of prevention based approaches detection based approaches are more important in MANET security. These methods play important role in MANET as MANET is having tremendous number of applications in real world.

References

[1]. Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Tech.*, vol. 61, no. 6, pp. 2674–2685, Jul. 2012.

[2]. F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and Quality of Service (QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J.Wireless Commun. Netw.*, vol. 2013, pp. 188–190, Jul. 2013.

[3]. Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, Mar. 2014.

[4]. J. Chapin and V.W. Chan, "The next 10 years of DoD wireless networking research," in *Proc. IEEE Milcom*, Nov. 2011, pp. 2155–2245

[5]. IEEE Std 802.11-2007, IEEE standard for information technology- Telecommunication and information exchange between systems- Local and metropolitan area network-Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications, June 2007

[6]. J. Loo, J. Lloret, and J. H. Ortiz, "*Mobile Ad Hoc Networks: Current Status and Future Trends,*"Boca Raton, FL, USA: CRC, 2011.

[7]. Jochen Schiller "Mobile Communications," Addison-Wesley, 2000.

[8]. P. Jacquet and L. Viennot, "Overhead in Mobile Ad-hoc Network Protocols," Research Report-3965, INRIA, France, June 2000. Available http://ftp.inria.fr/INRIA/publication/publi-ps-pz/RR/RR-3965.pz.gz

[9]. C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," presented at the 2nd OLSR Interop/Workshop, Palaiseau, France, Dec., 2005.

[10]. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable SecureComput.*, vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.

[11]. Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Comm.*, vol. 16, no. 2, pp. 24–30, Apr. 2009.

[12]. F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Trans.Netw. Serv. Manag.*, vol. 7, no. 4, pp. 258–267, Dec. 2010.

[13]. D. Dhillon, T. Randhawa, M. Wang, L. Lamont, "Implementing a Fully Distributed Certificate Authority in an OLSR MANET", WCNC 2004 IEEE, Atlanta, Georgia, USA

[14]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Proc. of IEEE/ACM MobiCom'00, pp. 255–265, Boston, MA, August 6-11, 2000.

[15]. M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use of public-key cryptography for multi-hop wireless networks", IEEE Transactions on Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[16]. M. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet drop in multihop wireless networks", IEEE Transactions on Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, 2011.

[17]. S. Zhong, J. Chen, and R. Yang, " Sprite: a simple, cheat-proof, credit based system for mobile ad-hoc networks", Proc. of IEEE INFOCOM'03, vol. 3, pp. 1987-1997, San Francisco, CA, March 30- April 3, 2003.

[18]. M. Mahmoud and X. Shen, "PIS: A practical incentive system for multi-hop wireless networks", IEEE Transactions on Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, 2010.

[19]. G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[20]. P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model," IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

[21]. S. Lindsay, Y. Wei, H. Zhu, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305- 317, Feb. 2006.

[22]. Shuaishuai Tan, Xiaoping Li, and Qingkuan Dong, "A Trust Management System for Securing Data Plane of Ad Hoc Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2015.

[23]. Stylianos Kraounakis, Ioannis N. Demetropoulos, Angelos Michalas, Mohammad S. Obaidat, Panagiotis G. Sarigiannidis, "A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015

[24]. Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 9, NOVEMBER 2014