Ad-Hoc Routing Protocols to Achieve Secure, Trust and Attacks-Proof

Kunjan Shrivastava[1], L.K Vishwamitra[2]
[1]*Mtech. Scholar,* [2]*Professor*
[1,2]*Department of Computer Science & Engineering, PCST, RGPV University, INDIA*

Abstract—Mobile Ad-Hoc networks (MANETs) are vulnerable to security threats due to the inherent characteristics of such networks, such as the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adversarial environments, such as battlefields. This article provides an overview of past and current work in the area of security research of mobile Ad-Hoc networks. Security is a critical issue in a mobile Ad-Hoc network (MANET). Securing network transmissions without securing the routing is not sufficient. In this, researchers have done review of selected of the distinctive types of Ad-Hoc networks, articulate difficulties and study research work completed in the region.

Keywords—MANET, Attacks, Security Protocols, security goals.

I. INTRODUCTION

We can inspect the multilevel data packets even with compressed data. MANET Network is prone to highly vulnerable attacks due to its dynamic nature of Network infrastructure, among these Routing attacks received considerable attention since entire MANET structure will collapse on routing failures or router snooping. Existing methods will result in Node isolation which leads to unexpected network partition which may backfire rather than protecting. The studies on node capture attacks have all focused on the ability of an adversary to compromise the security of single-hop wireless links. However, messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing a single insecure link. The overall security of routed messages is thus dependent on the routing protocol implemented in the wireless network, as well as the physical network topology and the relative positions of the source and destination nodes in the network. Moreover, the fact that a message is transmitted over numerous links between a source and destination node implies that the overall confidentiality and integrity of the routed message may only be as secure as the least secure link, implying that vulnerabilities arise due to the topology of secure links in the wireless network. Hence, the impact of a node capture attack is a function of both the cryptographic protocol which provides link security and the routing protocol which determines the set of links traversed by a given message. Mobile Ad-Hoc Network (MANET) are a class of wireless communication networks without a fixed infrastructure. The MANET concept basically evolved to tackle disaster situation like tsunami, earthquake, terrorist activities, battlefields, landslides, etc. Later, the concept has been extended to include applications such as online education, gaming, business, etc. Several applications in MANETs need group communication to manage the scenario. MANET nodes don't offer dependable services & QoS (Quality of Service) guarantees as compared to other wireless networks e.g. Wi-Fi, GSM ,Wi-MAX & CDMA.

The key sources of irregularity in MANETs are due to limited battery capability, inadequate memory and dealing out power, unstable channel conditions, less stability under unpredictable and high mobility of nodes. The QoS parameters to be guaranteed for multimedia group communication are spectrum, packet loss, delay, jitters and bandwidth-delay product. Ad-Hoc networks consist of hosts interconnected by routers without a fixed infrastructure and can be arranged dynamically. Considerable work has been done in the development of routing protocols in different types of Ad-Hoc networks like MANETs, WMNs, WSNs, and VANETS etc [1]. In recent years, the interest in Ad-Hoc networks has grown due to the availability of wireless communication devices that work in the ISM bands. While designing an ad hoc network in particular we are concerned with the capabilities and limitations that the physical layer imposes on the network performance. Since in wireless networks the radio communication links are unreliable so it is desirable to come up with an integrated design comprising of physical, MAC and network layers[2]. The main vision of MANET is to support robust and efficient operation in wireless networks by incorporating routing functionalities at each mobile node.

For such designing aspects of Ad-Hoc networks Routing based approach, Information-theoretic method, Dynamic control method or Game- theoretic method has been implemented [3].

In MANET to support mobile computing a mobile host must be able to communicate with other mobile hosts which may not lie within its radio transmission range. Hence routing protocols will need to perform four important functions as determination of network topology, maintaining network connectivity, transmission scheduling and channel assignment, and packet routing. Routing protocols in MANETs were developed based on the design goals of minimal overhead control, minimal dealing overhead, multi hop routing, dynamic topology protection and loop prevention [1].

II. SECURITY CONSIDERATIONS

We aim at achieving a security enhanced MANET protocol that fulfils the following main objectives. The objectives mitigate threats that are relevant in practice. The proposed concept is described in subsequent chapters.

Protection of communication channels:

In MANETs, communication between wireless devices is realized via an open broadcast medium. Compatible devices, in the range of a sending device are capable of receiving all contents of the transmission. Furthermore, they are capable of sending similar or equal contents on the medium. So far, security was not in the focus of the design of these networks. The proposed concept implements mechanisms for the protection of communication channels. It achieves confidentiality of all transmitted data on a hop-by-hop (direct link) basis and it protects from eavesdropping. Authentication and integrity assessment of a remote device precedes any data transmission. Protected communication channels are established in the field. All devices within transmission range exchange shared secrets for the protection of transmissions. The key exchange mechanism also uses the TPM whereby hardware protection against man-in the-middle -type threats is achieved.

Protection of privacy:

The provided solution protects the privacy of users of a device against peers. Unintended traceability, recognition and assignment of single device, and thereby its user, is confined to the link-layer. Pseudonymous TPM keys, the secured key exchange and transmission mechanisms support the protection of privacy. Solutions on higher and lower communication layers, as well as revealing device uniqueness, are not in heart of this effort. Cross layer security is e.g. discussed in [4].

Protection of routing tables:

Routing tables have to be protected from malicious manipulation in order to counter a variety of threats. Unsecured MANETs suffer from outside and inside attacks, pointing to insert wrong routing data (e.g. black hole, loops). The distribution of unkindly manipulated routing data should be prohibited. For our answer it is assumed that devices with a correct software state do not manipulate routing information maliciously. Thus, attacks either come from outsider devices or from manipulated software on known devices. The TPM and its integrity measurement mechanisms allow devices to recognize manipulations of neighbouring devices. Routing messages of manipulated devices are dropped and not forwarded in the network.

Protection of cryptographic keys:

Capturing of devices by an adversary is a serious concern for mobile equipment. Especially, pre-shared keys need to be protected even if devices are stolen. The provided solution does not require any pre-shared and MANET-wide symmetric keys which are expected to increase the vulnerability of the whole network. Instead it relies on asymmetric keys stored in the TPM. Identity keys and storage keys cannot be compromised by software means. Physical manipulations to TPMs are possible but difficult, expensive and time consuming. All other cryptographic keys utilized in the communication between devices are freshly created, bound to a well known system state and of short temporal validity.

III. TRUST IN MANET

Trust is a very acute feature that be influenced by on indeterminate situations and is used for judgment building on collaborating with strange members. It comprises creation and updation of trust. In overall, trust administration and status administration are always used but it is not always the fact. There always lies a variance between the trust and reputation.

Golbeck [5] explains nearly three main assets of trust in order to social network. Trust could not be

totally transitive in terms of mathematical. For example, if X trusts Y, and Y trusts Z, it does not guarantee that X trusts Z.

IV. ROUTING ATTACKS IN MANET

There are various means and ways to attacks in MANET by malicious node(s), for example, sending false messages numerous times, false routing data, and promoting false links to disorder routing actions. Various routing attacks against MANET [5] protocols are deliberated in brief. Here some of the critical and vital routing attacks are taken in consideration.

4.1 Flooding attack

Attacker is meant for exhausting the mobile Ad-Hoc network's all resources, for example bandwidth and other resources of a node, for example computational efforts and battery energy or to interrupt the routing main operations to reason undecorated degradation in performance of network. Such as , AODV[6] protocol, any malicious node could spread huge number of RREQs in a very short span of time to a target node which does not exist actually in the network. For this situation, no node would reply to this RREQs, and finally these request, RREQs, would flood the whole Ad-Hoc network. In the result form, all of the nodes of Ad-Hoc network get overwhelm with battery power and network bandwidth of network would be spent and could prime to denial-of service.

4.2 Blackhole attack

A black hole is created with the opponent at the main centre. The opponent traps the traffic of the network close to a compromised in this type of attack. Basically the attacker offers an attractive path to the neighboring nodes. This attack can also be paired with other attacks like packets dropping, denial of service, replay of knowledge, selective forwarding [7].

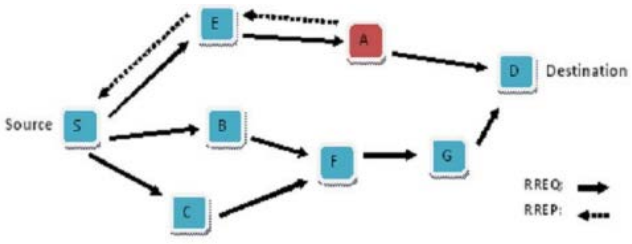

Fig 1: Blackhole Attack in AODV

4.3 Link spoofing attack

This is a attack where a malicious node broadcast false links with all those nodes which are not direct neighbors of the node to interrupt routing operations. Such as, in the OLSR, an attacker could spread a false link with a all those nodes which have target's two-hop neighbors. And undoubtedly, this serious reasons the group of target nodes to choice the malicious node, which is to be its own MPR[7].

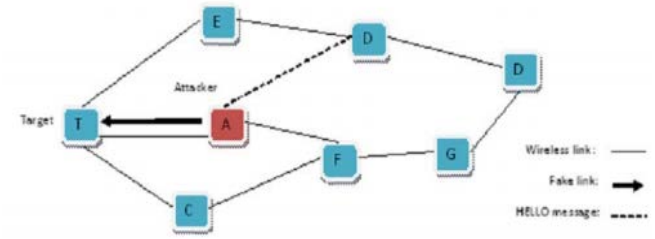

Fig 2: Link Spoofing Attack

4.4 Wormhole attack

Here the opponent connects two distant parts of the network and convey messages received in different part of the network to the extra. A minor latency link is used to exceed the messages in this type of network [7].

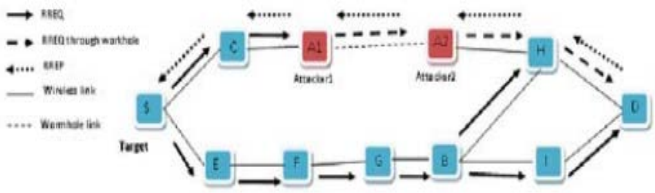

Fig 3: Worm whole Attack on reactive routing

V. ROUTING PROTOCOLS

In this section, we introduce the basic concepts in anonymous routing, and provide a short survey on the existing routing protocols.

A. Anonymity and Security Primitives

We begin some general mechanisms that are broadly used in anonymous secure routing.

1) *Trapdoor: A* trapdoor is a concept which defines a one-way working function between 2 sets [8]. Information is collected by global trapdoor. In this global trapdoor each

intermediate nodes add some information, i.e. node IDs. Source and destination are the nodes which could unlock these and retrieve using secret keys.

2) *Onion Routing:* It is a mechanism to provide private communications over a public network [9]. The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route demand message. The starting place and target nodes do not essentially know the ID of a forwarding node. The target node receives the onion and delivers it along the route back to the starting place. The transitional node can validate its role by decrypting and deleting the external layer of the onion. Ultimately an unidentified route can be recognized.

3) *Group Signature:* It is a scheme [10] which can provide authentications and this could happen without troubling the inconspicuousness. Each and every member of the group have a pair of group private and public keys. And this group is delivered by the group trust authority (such as, group manager).

B. Anonymous On-demand Routing Protocols

There are many anonymous on-demand routing protocols. Similar to the Ad-Hoc routing, there are two categories: topology-based and location-based [12], or in other words, node identity centric and location centric [11]. We compare the protocols in Table I, in terms of the key distribution assumption, node anonymity in route discovery, and packet authentication. Our observations are summarized as follows:

First of all, the routing protocols are designed to work in different scenarios. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services. Since ours is for general MANETs, we focus on the topology-based routing rather than location-based routing.

Secondly, as mentioned in Section I, SDAR, AnonDSR, MASK, and D-ANODR have problems in meeting the unindentifiability and unlink ability. The node IDs in a neighbourhood and along a route are possibly exposed in SDAR and AnonDSR, respectively. The plain node IDs are used in the route request of MASK and D-ANODR. In this work, we use the node's pseudonym instead of its real ID, to avoid the information leakage during RREQ and RREP processes.

Thirdly, some of the protocols adopt additional authentication schemes to sign the routing packets, including A3RP, RAODR [13], USOR [14], and PRISM [15]. Note that, although MASK provides neighbourhood authentication, it cannot sign the routing packets. RAODR form a master key mechanism, which cannot provide the mystery, enforceability and traceability that are supported by a group signature. A3RP and USOR adopt a group signature and use secure hash functions to map the keys and node pseudonyms along a route. We choose the onion based routing to record the anonymous routes, because the onion is more scalable than other mechanisms and can be complete, for example to many paths.

Fourthly, we need to rethink the assumptions on the key distribution and node anonymity in route discovery. For example, ARM assumes that the source and destination nodes share a long-term session key in advance, which is not practical for real-world MANETs. We assume that the nodes are equipped with public and private keys during network initialization phase and can generate the shared symmetric key in an on demand manner.

VI. CONCLUSIONS AND FUTURE WORK

In recent years the widespread availability of wireless infrastructure, mobile computing and handheld devices has led to the development and significance of wireless mobile Ad-Hoc networks. Though there have been many works in the recent years on security issues in MANET. The issues involved in privacy preservation in MANET can be resolved by implementing trust coefficient. Our concept of trust management is intended to ensure trust in participating nodes of MANET and also applies not only to mobile networks but to distributed infrastructure-less networks as well. The Packet Drop Attack amongst the nodes is not adequately addressed and there is the opportunity to work on this emergent issue related to prevent and eliminate the packet dropping attacks.

This study motivates us to do further work in the area of security routing protocol.

REFERENCES

[1] Kannhavong B, Nakayama H, Nemoto Y, Kato N, and Jamalipour A, "A Survey of Routing Attacks in Mobile Ad-HocNetworks,"IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[2] Marti S, Giuli T, Lai K, and Baker M,"Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks,"Proc. ACM MobiCom,pp. 255-265,2000.

[3] Hu Y, Johnson D, and Perrig A, "SEAD: Secure EfficientDistanceVector Routing for Mobile Wireless Ad-Hoc Networks," Ad-Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[4] Kidston, L. Li, H. Tang, and P. Mason, "Mitigating security threats in tactical networks," in IST Panel Symposium, Military Communication and Networks, 2010, Wroclaw, Poland.

[5] Marti S, Giuli T, Lai K, and Baker M,"Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks,"Proc. ACM MobiCom,pp. 255-265,2000.

[6] Perkins C, Belding-Royer E, Das S, Ad-Hoc On-demand Distance Vector(AODV)Routing,Draft-ietf-manet-aodv-11.txt, June2002 (work in progress).

[7] Weichao Wang, Yi Lu, Bharat Bhargava, "On Security Studyof Two Distance Vector Routing Protocols for Mobile Ad-Hoc Networks",(IEEE) 2003, 0-7695-1893- 1/03.

[8] S. William and W. Stallings, *Cryptography and Network Security, 4th Edition*. Pearson Education India, 2006.

[9] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE Journal on Selcted Area in Communication.*, vol. 16, no. 4, pp. 482–494, May 1998.

[10] Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Int. Cryptology Conf. (CRYPTO'04), Aug. 2004.

[11] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," *IEEE Trans. On Mobile Computing*, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.

[12] Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks," in Proc. IEEE WCNC'09, Apr. 2009.

[13] R. Song and L. Korba, "A robust anonymous Ad-Hoc on-demand routing," in *Proc. IEEE MILCOM'09*, Oct. 2009.

[14] Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure OnDemand Routing Protocol for Mobile Ad-Hoc Networks," *IEEE Trans. on Wireless Communication*, vol. 11, no. 5, pp. 1922–1932, May. 2012.

[15] K. E. Defrawy and G. Tsudik, "Privacy-Preserving Location-Based On Demand Routing in MANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.