International Journal of Computing Communication and Information System(IJCCIS)
Vol.6. No.3 – July-September 2014 Pp. 128-132
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

A STUDY ON SECURITY IN MOBILE ADHOC NETWORK

T.Balasubramanian
Dept. of Comp. Sci
Sri Vidya Mandir Arts and Science College
Uthangarai, Krishnagiri(Dt.)
balaeswar123@gmail.com

ABSTRACT

Secure communication between two nodes in a network depends on reliable key management systems that generate and distribute keys between communicating nodes and a secure routing protocol that establishes a route between them. But due to lack of central server and infrastructure in Mobile Ad hoc Networks (MANETs), this is major problem to manage the keys in the network. Dynamically changes in network's topology causes weak trust relationship among the nodes in the network. . In MANETs a mobile node operates as not only end terminal but also as an intermediate router. Therefore, a multi-hop scenario occurs for communication in MANETs; where there may be one or more malicious nodes in between source and destination. A routing protocol is said to be secure that detects the detrimental effects of malicious node(s in the path from source to destination). In this paper, we proposed a key management scheme and a secure routing protocol that secures on demand routing protocol such as DSR and AODV.

Index Terms —***MANET, Group, Key management, Secure Routing, Security, Authentication, Integrity, Non-repudiation, Confidentiality, Key and Trust Management, and Access Control.***

1 INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example:
initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F.

2. GROUP FORMATION

Grouping or clustering is a process that divides the network into interconnected substructure known as groups. Grouping provides a better solution to the problem of key management and routing in MANET. There is a group leader as coordinator in every group. Each group leader acts as a temporary base station within its zone or group and communicates with other group leader. A system model of open MANET is shown in Figure.1. Mobile nodes are divided into several groups in such a way that all the nodes are covered with no groups overlapped. Some of the nodes are selected as group leaders to perform the functions of key management system and other administrative functions in its group. Aim of constructing the grouped based structure is that grouping preserves the structure of network as long as possible, when nodes moves or topology is slowly changing. On the other hand, grouping reduces the number of keys, required to distribute in network for secure communication. Group based structure distributes the functions of a central server into several nodes (group leaders). Therefore, it combines both centralized and distributed approaches of key management system providing a decentralized solution. Group based structure of networks also removes the vulnerability of

compromising single central server. If a group leader is compromised; only a group will be compromised leaving rest of the network safe and secure.

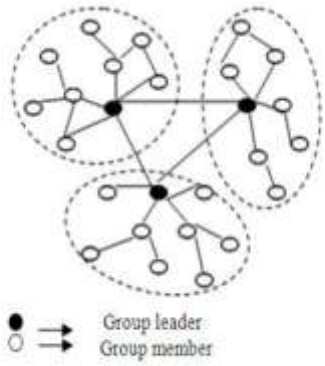

Figure 1. System model for MANET

3. ROUTING PROTOCOLS FOR MANETS

Research on MANETs has nearly 20 years focused on routing and this focus still remains. Several routing protocols for MANETs have been proposed and some surveys on these protocols have been published (Feeney, 1999; Qin & Kunz, 2004; Liu & Kaiser, 2005; Taneja & Kush, 2010) and an IETF Routing Area Working Group MANET (Mobile, 2011) has been active for a decade with six currently active Internet drafts.

Routing protocols for MANETs are usually classified into table driven/proactive protocols, on-demand/reactive protocols, and hybrid protocols based on how routing information is acquired and maintained by mobile nodes. Table driven/proactive protocols use a proactive routing scheme, in which every network node maintains consistent up-to-date routing information from each node to all other nodes in the network. On-demand/reactive protocols are based on a reactive routing scheme, in which at least one route is established only when needed. A hybrid routing protocol is a combination of proactive and reactive schemes with the aim of exploiting the advan-tages of both types of protocols. (Qin & Kunz, 2004; Liu & Kaiser, 2005; Abusalah, Khokhar & Guizani, 2008; Singh, 2011)

Another classification into uniform and non-uniform routing protocols for MANETs is based on the network node roles in a routing scheme. In a uniform routing protocol all network nodes have the same role, importance and functionality. In a non-uniform routing protocol some network nodes carry out distinct management and/or routing functions. A uniform routing protocols is ei-ther reactive or proactive, while different classification schemes have been proposed for non-uniform routing protocol (Feeney, 1999; Liu & Kaiser, 2005)

In this section some relevant reactive, proactive, and hybrid routing protocols for MANETs are presented.

1) ***On Demand/Reactive Protocols***
2) ***Table Driven/Proactive Protocols***

4. DYNAMIC SOURCE ROUTING (DSR)

As with AODV, DSR floods the network with route request messages as a result of route discov-ery initiation. However, compared with AODV, the destination node returns a route reply for each copy of route request message it receives. As a result, the source node will know more than one route to the destination node upon reception of all route replies. The addresses of all nodes through which both route request and route reply messages have traversed are added to the rout-ing message headers, so a node knows not only the hop count values of all routes to a destination, but also all the intermediate nodes. Based on hop count and other route information, the source node finally selects the route with the lowest latency. Each data packet carries, in its header, the complete ordered list of intermediate nodes through which a packet is to be transmitted.

DSR has lower network overheads compared with AODV, mainly due to the multiple storage and source routing features. If a link fails, the source node does not need to re-initiate route discovery, as in AODV. Instead it selects another route from its routing table. Since the route information is included in all data packets, other nodes forwarding or overhearing any data packet can cache the routing information for future use, which also eliminates the need for route discovery if the route is still fresh.

5. SECURE ROUTING PROTOCOLS FOR MANETS

Most routing protocols have been designed without taking security into account. It has been as-sumed that all nodes in a MANET are trusted. However, this is not the case in a large scale and dynamic MANET and if the routing protocol is unprotected, the whole MANET can be liable to several different types of security attacks. Much research has been done in the area of routing se-curity in MANETs and several surveys on this research

have been published (Abusalah, Khokhar & Guizani, 2008; Wang, Hu & Zhi, 2008; Djenouri & Badache, 2010; Singh, 2011). Due to the dominant status of reactive routing protocols for MANETs, most security research has tended to give attention to these protocols.

1. A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.
2. Trust should be determined in a highly customizable manner without excessive computa-tion and communication load, while also capturing the complexities of the trust relation-ship.
3. A trust decision framework for MANETs should not assume that all nodes are coopera-tive. In resource-restricted environments, selfishness is likely to be prevalent over coop-eration, for example, in order to save battery life or computational power.
4. Trust is dynamic, not static.
5. Trust is subjective.

5. TRUST BASED SECURE ROUTING

In this subsection, the three trust-based MANET routing protocols: QoS Route Discovery, Confi-dant and TAODV are reviewed. An overview of trust-based routing schemes in MANETs is pro-vided in (Patmaik & Gore, 2011).

6. COOPERATION OF NODES: FAIRNESS IN DYNAMIC AD HOC NETWORKS (CONFIDANT)

The main idea of Confidant (Buchegger & Boudec, 2002) is to make non cooperative nodes unat-tractive for other nodes to communicate with. A node chooses a route based on trust relationships built up from experienced, observed or reported routing and forwarding behavior of other nodes. Each node observes the behavior of all nodes located within the radio range. When a node dis-covers a misbehaving node, it informs all other nodes in the network by flooding an alarm mes- sage. As a result, all nodes in the network can avoid the detected misbehaving node when choos-ing a route.

Thus Confidant effectively detects non cooperative nodes such as selfish nodes and PM worm-hole nodes that drop data packets. HM wormhole nodes and PM wormhole nodes that do not drop packets are, however, not detected. Moreover, a major weakness of Confidant is that an attacker is able to send false alarm messages, and as a consequence the attacker can claim that a node is misbehaving even if that is not true.

7. TRUSTED AODV (TAODV)

In TAODV route selection is based on quantitative Route Trust and Node Trust values (Pushpa, 2009; Pirzada & McDonald, 2004).

Route Trust from a source node to a destination node is defined as the difference between the number of packets sent from the source node and the number of related packets received by the destination node. Route Trust is thus 0 for a perfect route and trustworthiness decreases for grow-ing Route Trust values.

For calculation of Node Trust each node monitors the behavior of all neighbor nodes by counting both successes and failures of events such as Control Packets Received, Control Packets For-warded, Data Packets Received, Data Packets Forwarded, Route Established etc. Node Trust val-ue for a certain monitored event type is *(Rs-Rf)/(Rs+Rf)*, where *Rs* and *Rf* are the number of suc-cessful and failed events respectively. This value will lie between +1 (complete trust) and -1 (complete mistrust). Node Trust for a neighbor node is weighted sum of the trust values for all monitored event types. The weights are dynamically assigned values between 0 and 1based on circumstances and chosen criteria.

For route selection RT = 0.4 * (Hop Count) + 0.6 * (Route Trust) and the 3 neighbor nodes are selected from which the routes with lowest RT values start. For each selected node an average Node Trust is calculated from the monitored Trust Values of neighbor nodes. The route starting from the node with the highest average Node Trust is selected.

8. QOS ROUTE DISCOVERY

In (Maltz, 1999) a QoS-Guided route discovery protocol for MANETs is presented. In this proto-col a node specifies route trust by traditional QoS metrics, bandwidth, latency and jitter that must be satisfied by a discovered route.

8.1 CRYPTOGRAPHY BASED SECURE ROUTING

In this subsection the cryptography-based secure routing protocols in Table 1 are presented.

SECURING QOS ROUTE DISCOVERY (SQOS ROUTE DISCOVERY)

SQoS Route Discovery (Hu & Johnson, 2004) is a cryptographically protected version of QoS Route Discovery. SQoS Route Discovery relies entirely on symmetric cryptography.

SECURITY AWARE AD HOC ROUTING (SAR)

The SAR protocol (Yi et al., 2001) incorporates security attributes as parameters into ad hoc route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criteria for a valid route can be that every node in the route must own a particular shared key. In such a case, routing messages would be encrypted with the source node's shared key and only the nodes with the cor-rect key can read the header and forward that routing message. As a result, if a routing message reaches the destination, it must have been traveled through nodes having the same trust level as the source node. It is then for the node initiating the route discovery to decide upon the desired security level for that route.

SAR has been presented as an extension to AODV but it can also be extended to any existing routing protocol. Due to strong cryptographic protection of routing messages, attacks such as modification, impersonation, and fabrication are effectively eliminated. A major problem with SAR, however, is that it involves significant encryption overhead since each intermediate node has to perform both encryption and decryption operations.

9. AUTHENTICATED ROUTING FOR AD HOC NETWORKS (ARAN)

The purpose of the ARAN protocol (Sanzgiri et al., 2002) is to detect and protect against mali-cious actions by third parties and peers. It provides authentication, message integrity, and non-repudiation. ARAN can be used in two different security stages: a simple mode which is manda-tory and an optional stage which provides stronger security but also more overhead and is not suitable on mobile devices with very low processing or battery capacity. ARAN uses crypto-graphic certificates for authentication and non-repudiation. Each routing message is signed by the source node and broadcasted to all neighbors. An intermediate node removes the certificate and signature of the previous hop and replaces them with its own.

Due to strong authentication, message integrity, and non –repudiation ARAN provides effective protection from modification, impersonation, and fabrication attacks. However, due to heavy asymmetric cryptographic operations and large routing packets, ARAN has a high computational cost for route discovery. ARAN is also vulnerable against selfish nodes that e.g. drop routing packets. In particular, if the selfish node is an authenticated node, then ARAN is unable to detect this type of attack.

10. SECURE EFFICIENT AD HOC NETWORKS (SEAD)

SEAD (Hu, Johnson, & Perrig, 2002b) is a proactive routing protocol based on DSDV. SEAD uses a hash chain method for checking the authenticity of data packets and the hash chain value is used for transmitting routing updates. The authentication of each entry of a routing update mes-sage is verified by a receiving node. Looping is removed by using a sequence number and authen-tication of the source of routing update message. Authentication of the source can be done for example by providing a shared secret key between each pair of nodes in the MANET which is then used for MAC calculations between the nodes for the authentication of a routing update message.

SEAD provides strong protection against attackers trying to create incorrect routing state in other nodes by for example modifying the sequence number in the routing packet. However, SEAD does not protect against an attacker tampering the next hop or the destination field of a routing update packet.

11. SECURE LINK STATE ROUTING PROTOCOL (SLSP)

The main functionality of SLSP (Papadimitratos &Haas, 2003) is to secure the discovery and the distribution of link state information by using asymmetric keys. SLSP consists of three major steps: public key distribution, neighbor discovery, and link state updates. Public keys are distrib-uted between a node and all its neighbors. A central server for key distribution is thus not needed. Periodic hello messages, used in neighbor discovery, are signed using the private key of the send-er. Signed link state update messages are identified by the IP address of the initiating node and include a sequence number. A node receiving a link update messages verifies the attached signa-ture using the public key it received earlier during the public key distribution phase. The hop count field in the update message is protected by using a one-way hash chain.

REFERENCES

1) Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. IEEE Communications Surveys & Tutorial, 10(4), 78-93.

2) Buchegger, S., & Boudec, J.-Y.L. (2002). Cooperation of nodes fairness in dynamic ad-hoc networks. Pro-ceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

3) Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol (OLSR). IETF, Request for Com-ments (RFC) 3626.

4) L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13, no. 6, pp: 24–30, 1999.

5) Meng Ge, Kwok-yan Lam, "Self-healing Key Management Service for Mobile Ad Hoc Networks",Proceeding of first International Conference on Ubiquitous and Future Networks", June, 2009.

6) S. Yi and R. Kravets, "MOCA: Mobile Certificate Authority for Wireless Ad hoc networks," 2nd Annual PKI Research Workshop (PKI 03), 2003.