Secure Anonymous Route Discovery Protocol for Ad Hoc Routing in Ad Hoc Wireless Networks

Mohammed Ali Hussain¹, Sarath Babu Duggirala²

¹Professor & Head, Dept. of CSE, Sri Sai Madhavi Institute of Science & Technology, Rajahmundry, A.P., India.
²Asst. Professor, Dept. of CSE, DJR group of Engineering, A.P., India.

alihussain.phd@gmail.com, sarath_duggirala@yahoo.com

Abstract - Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There are various challenges that are faced in the Ad-hoc environment. These are mostly due to the resource poorness of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. Ad-hoc networks therefore throw up new requirements and problems in all areas of networking. The solutions for conventional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. One of the important issue is that an ad hoc wireless network permits wireless mobile nodes to communicate without prior infrastructure. Due to the limited range of each wireless node, communication sessions between two nodes are usually established through a number of intermediate nodes. Unfortunately, some of these intermediate nodes might be malicious, forming a threat to the security or confidentiality of exchanged data. While data encryption can protect the content exchanged between nodes, analysis of communication patterns may reveal valuable information about end users and their relationships. Using anonymous paths for communication provides security and privacy against traffic analysis. To establish these anonymous paths, all nodes build a global view of the network by exchanging routing information. In this paper we focus on Ad hoc routing and we present a secure anonymous route discovery protocol for Ad hoc routing in Ad hoc wireless networks.

Keywords – Ad- hoc network, Ad- hoc routing, Route discovery protocol.

1. Introduction

On wireless computer networks, ad hoc mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to peer fashion without involving central access. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wired Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other’s radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems [1] [2]. Figure 1 shows the working of ad hoc network.
There are two different types of wireless networks. The first and easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes “can see” the others. The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

An ad hoc wireless network is a collection of wireless mobile nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Ad hoc networks use mobile nodes to enable communication outside wireless transmission range. There are a number of circumstances where an ad hoc network is advantageous in the absence of network infrastructure. Examples of such circumstances include: battlefields where each soldier might be carrying a wireless transceiver; or on-the-fly conference environments where devices used by attendees collaborate to enable end-to-end communication between attendees, and perhaps Internet connection, without the requirement of a wireless infrastructure. In some environments, such as the military environment or even emergency/rescue environments, the information exchanged between two communicating parties might include highly sensitive data that must be secured when sent through intermediate nodes. While end-to-end security mechanisms can provide security for the data, valuable information regarding the nature and location of communicating entities may be determined from traffic analysis and routing data transported in the clear. Network-based anonymity techniques offer the prospect for hiding this information.

For the Internet, several network-based anonymity approaches provide anonymous communication between end-nodes. These approaches include DC-nets [3], Crowds [4], MIX networks [5], and Onion Routing [6]. Both MIX networks and Onion Routing share the same concept of establishing an anonymous path for the data transfer. To construct the anonymous path, a source node must store and maintain information about the topology of the network. Keeping up-to-date information about the topology of the network is complex in the absence of fixed infrastructure and in the presence of dynamic topology, as found in ad hoc wireless environments. In this paper we focus on Ad hoc routing and we present a secure anonymous route discovery protocol for Ad hoc routing in Ad hoc wireless networks.

2. Ad- hoc routing and the problems associated with it

2.1 Infrastructure

An Ad-hoc network is an infrastructure less network. Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end-to-end routing. The nodes themselves are responsible for routing packets. Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them. Figure 2 shows the routing in both traditional and ad hoc networks.
2.2 Frequent changes in network topology

Ad-hoc networks contain nodes that may frequently change their locations. Hence the topology in these networks is highly dynamic. This results in frequently changing neighbors on whom a node relies for routing. As a result traditional routing protocols can no longer be used in such an environment. This mandates new routing protocols that can handle the dynamic topology by facilitating fresh route discoveries.

2.3 Problems associated with wireless communication

As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems.

2.4 Problems with existing Ad-hoc routing protocols

2.4.1 Implicit trust relationship between neighbors

Current Ad-hoc routing protocols inherently trust all participants. Most Ad-hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets. This naive trust model allows malicious nodes to paralyze an Ad-hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad-hoc environment magnifies this makes detection difficult.

2.4.2 Throughput

Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high.

![Fig 3. Attack by a malicious node M](image)

2.4.3 Attacks using modification of protocol fields of messages

Current routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields.

For example, in the network illustrated in Figure 3, a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X, which C is advertising.

The attacks can be classified as remote redirection attacks and denial of service attacks. Let us look at them now.

(a) Remote redirection with modified route sequence number (AODV)

Remote redirection attacks are also called black hole attacks. In the attacks, a malicious node uses
routing protocol to advertise itself as the shortest path to nodes whose packets it wants to intercept. Protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes towards a specific destination. In AODV, any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value.

Figure 3 illustrates an example ad hoc network. Suppose a malicious node, M, receives the RREQ that originated from S for destination X after it is re-broadcast by B during route discovery. M redirects traffic towards itself by unicasting to B a RREP containing a significantly higher destination sequence num for X than the authentic value last advertised by X.

(b) Redirection with modified hop count (AODV)

A redirection attack is also possible in certain protocols, such as AODV, by modification of the hop count field in route discovery messages. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes can attract route towards themselves by resetting the hop count field of the RREP to zero. Similarly, by setting the hop count field of the RREP to infinity, routes will tend to be created that do not include the malicious node.

Once the malicious node has been able to insert itself between two communicating nodes it is able to do anything with the packets passing between them. It can choose to drop packets to perform a denial of service attack, or alternatively use its place on the route as a first step in man-in-the-middle attack.

(c) Denial of service with modified source routes

DSR is a routing protocol, which explicitly states routes in data packets. These routes lack any integrity checks and a simple denial-of-service attack can be launched in DSR by altering the source routes in packet headers. Modification to source routes in DSR may also include the introduction of loops in the specified path. Although DSR prevents looping during the route discovery process, there are insufficient safeguards to prevent the insertion of loops into a source route after a route has been salvaged.

2.5 Attacks using impersonation

Current Ad-hoc routing protocols do not authenticate source IP address. A malicious node can launch many attacks by altering its MAC or IP address. Both AODV and DSR are susceptible to this attack.

2.6 Attacks using fabrication

Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

2.6.1. Falsifying route error messages in AODV or DSR

AODV and DSR implement path maintenance measures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the node upstream of the link break broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. The vulnerability is that routing attacks can be launched by sending false route error messages. Suppose node S has a route to node X via nodes A, B, and C, as in Figure 3. A malicious node M can launch a denial of service attack against X by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and X. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for X and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to X, M can successfully prevent communications between S and X.

2.6.2. Route cache poisoning in DSR

This is a passive attack that can occur in DSR due to promiscuous mode of updating routing table which is employed by DSR. This occurs when information stored in routing table at routers is deleted, altered or injected with false information. In addition to learning routes from headers of packets, which a node is processing along a path, routes in DSR may also be learned from promiscuously received packets. A node overhearing any packet may add the routing information contained in that packet's header to its
own route cache, even if that node is not on the path from source to destination.

The vulnerability is that an attacker could easily exploit this method of learning routes and poison route caches. Suppose a malicious node M wanted to poison routes to node X. If M were to broadcast spoofed packets with source routes to X via itself, neighboring nodes that overhear the packet transmission may add the route to their route cache.

2.6.3. Routing table overflow attack

In routing table overflow attack, the attacker attempts to create route to non-existent nodes. The goal of the attacker is to create enough routers to prevent new routes from being created or overwhelm the protocol. Implementation and flush out legitimate routes from routing tables. Proactive routing algorithms attempt to discover routing information even before they are needed, while reactive algorithms create only when they are needed. This makes proactive algorithms more vulnerable to table overflow attacks.

3. Secure Anonymous Route Discovery Protocol for Ad Hoc Routing

In this section, we present our anonymous route discovery protocol for establishing anonymous path in ad hoc wireless networks. The major objective of the protocol is to allow intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes.

3.1 Overview

To send data anonymously to a receiver node R, a Sender node S has to discover and establish an anonymous path that connects the two nodes. Both the path discovery and establishment process should be carried out without jeopardizing the anonymity of the communicating nodes. Our approach presented here for constructing the anonymous path is based on the DSR [7] protocol and can replace it for anonymous communication in ad hoc networks. The process is divided into two phases: the path discovery phase and the path reverse phase. Distributed information gathering about intermediate nodes that can be used along an anonymous path is carried out during the path discovery phase, while passing this information to the source node takes place during the path reverse phase.

3.2 Notations and Terminologies

Notations and terminologies are defined as follows.

- \( ID_i \): identity of node i, e.g. \( ID_R \) is the identity of the receiver R.
- \( PK_i \): public key of node i, e.g. \( PK_S \) is the public key of the receiver R.
- \( TPK \): a temporary one-time public key.
- \( TSK \): the private (secret) key corresponding to \( TPK \).
- \( K_i \): symmetric (session) key generated by node i, e.g. \( K_S \) is the symmetric (session) key generated by the source node S.
- \( PLS \): the padding length set by the sender.
- \( PS \): a padding implemented by the sender.
- \( PLS_r \): the padding length made by the receiver node R.
- \( PK_r \): a padding made by the receiver node R.
- \( E(M) \): The message M is encrypted with a public key \( PK_i \), e.g. RSA.
- \( (K,E(M)) \): The message M is encrypted with the symmetric key \( K_i \), e.g. DES.
- \( H(M) \): The message M is hashed with a hash function, e.g. MD5.
- \( Signs(M) \): The message M is signed with the source node S's private key, e.g. RSA.
- \( SN_{session, ID_i} \): A random number generated by node \( ID_i \) for the current session.

3.3 Path Discovery Phase

The path discovery phase allows a source node S that wants to communicate securely and privately with node R to discover and establish a routing path through a number of intermediate wireless nodes. An important characteristic of this phase is that none of the intermediate nodes that participated in the route discovery phase can discover the identity of the sending node S and receiving node R.

The source node S triggers the path discovery phase by sending a path discovery message to all nodes within its wireless transmission range. The path discovery message has four parts. The first part is the open part. It consists of a one-time public key \( TPK \), which is generated for each route discovery session and used by each intermediate node to encrypt routing information appended to the path discovery message. This key serves also as a unique identifier for the message. The second part contains the identifier \( IDR \) of the intended receiver, and the symmetric key \( K_S \) generated by the source node, all encrypted with the public key \( PK_R \) of the receiver. The source node may learn about the
public key $PK_R$ of the destined receiver through a number of ways including using the service of a certificate authority (CA). The symmetric key $KS$ is used to encrypt the third part of the message as well as to protect against replay attacks. The third part consists of $IDS$, $PKS$, $TPK$, $TSK$, $SN\text{ }Session\_IDS$ $PLS$, $PS$, and $SignS(MS)$, all encrypted with $KS$. The intended receiver uses the public key $TPK$ and it corresponding private key $TSK$ to decrypt and verify the routing information in the message. $SN\text{ }Session\_IDS$ is a random number generated by the source node and is mapped to the encryption key $KS$ to use with which message. The padding $PS$ protects against message size attack, and: $SignS$ protects the integrity of the message. The fourth part of the message holds information about intermediate nodes that have already handled the message, as described below. Therefore, a message sent by a source node has the following format (fourth part not yet available):

$$TPK, EPK_{K_S}(IDS, KS), E_{KS}(IDS, PKS, TPK, TSK, SN\text{ }Session\_IDr, PLS, PS, SignS(MS))$$

where $M_S = H(TPK, TSK, IDr, KS, IDS, PKS, SN\text{ }Session\_IDr, PLS, PS)$.

We assume that each node keeps an internal table for mapping the randomly generated number of a session to the encryption key for the session, as well as to the ancestor and successor node along the anonymous path for the session. Given an encrypted message and a randomly generated number, a node can use this mapping table to know which key to use to encrypt the message as well as the ID of the node to which to forward the message. Only the random number, session key, and ancestor node entries are added to the table during the path discovery phase, while the successor node entry is added later during the path reverse phase.

### 3.4 Path Reverse Phase

The path discovery message is forwarded from one node to the other in the network until it reaches the target receiver $R$, which triggers the path reverse phase. When the intended receiver gets the path discovery message, it can use its private key to retrieve $KS$. Then using $KS$, it can obtain the temporary private (secret) key $TSK$ encrypted in the third part of the message. Using $TSK$, the receiver node $R$ can also retrieve the id’s of all intermediate nodes and the session key to use with each one of these intermediate nodes, and the random number generated by each node. The receiver then composes a message that contains all these random numbers and the corresponding session keys, and encrypts the message with the session keys of all the nodes along the path to the source node. With each encryption, the receiver $R$ adds a layer that contains the random number generated by the node along the reverse path to the sender. If the first node to get this message from the receiver is node $i$, the encrypted message constructed by the receiver $R$ will have the following format:

$$Eki(…..(Eki(Eksi(SN\text{ }Session\_IDr, K1, SN\text{ }Session\_ID2, K2, …, Ki, SN\text{ }Session\_ID3), SN\text{ }Session\_ID4), SN\text{ }Session\_ID5), SN\text{ }Session\_ID6)…), SN\text{ }Session\_ID7)$$

Each intermediate node that receives the path reverse message uses the $SN\text{ }Session\_IDi$ to retrieve the key for the session, removes one encryption layer and forwards the message to the next node on the reverse path to the source node. The ID of the node from which the message was received is added to the successor node entry corresponding to the random number into the mapping table. When the source node receives the message, it decrypts the message and passes the information about all the intermediate nodes (i.e.: the route) to the higher application.

#### 3.5 Data Transfer Phase

The path reverse message is forwarded from node to node along the path that the receiver chooses, until it reaches the original sender $S$, which triggers the data transfer phase. After the sender gets the path reverse message, it first checks whether or not the message is correct, and then uses the shared session keys of the intermediate nodes to make the following layer encryption for the data (Data), which the sender wants to transfer to the receiver.

$$Eki(Ek(K1(…..Ek(SN\text{ }Session\_IDi), SN\text{ }Session\_IDi-1))$$

Each intermediate node just decrypts one encryption layer and forwards the message to the next node according to the id of the next node.

### 4. Conclusion

An ad hoc wireless network permits wireless mobile nodes to communicate without prior infrastructure. Due to the limited range of each wireless node, communication sessions between two nodes are usually
established through a number of intermediate nodes. Unfortunately, some of these intermediate nodes might be malicious, forming a threat to the security or confidentiality of exchanged data. While data encryption can protect the content exchanged between nodes, analysis of communication patterns may reveal valuable information about end users and their relationships. Using anonymous paths for communication provides security and privacy against traffic analysis. To establish these anonymous paths, all nodes build a global view of the network by exchanging routing information. This paper focuses on Ad hoc routing and we present a secure anonymous route discovery protocol for Ad hoc routing in Ad hoc wireless networks. The protocol provides an adequate level of security and anonymity for the sender and receiver during path establishment.

References


AUTHORS PROFILE

Mohammed Ali Hussain working as Professor & Head Dept. of Computer Science & Engineering at Sri Sai Madhavi Institute of Science & Technology, Mallampudi, Rajahmundry, A.P., India. His research interests include Wireless Networks, Mobile Networks and Web Commerce. He has published large number of papers in National & International Conferences and International journals. He also served as a Program Committee (PC) Member for many International Conferences. He is at present Chief Technical Advisory Board Member, Chief Editor, Editor and Reviewer of many International journals. He is a member of International Association of Engineers, IACSIT, IRACST and ISTE.

Sarath Babu Duggirala working as Asst.Professor in Dept. of CSE at DJR group of Engineering, A.P., India. His research interests includes Computer Networks, Wireless Networks and Ad Hoc Networks.