SECURED PREEMPTIVE DSR(S-PDSR): AN INTEGRATION OF SRP AND SMT WITH PREEMPTIVE DSR FOR SECURED ROUTE DISCOVERY

Ramesh.V [1], Dr.P.Subbaiah [2]
[1]Research Scholar, Sathyabama University, Chennai, INDIA
[2]Professor & Head, Narayana Engg. College, Nellore, AP, INDIA
E-mail : [1]v2ramesh634@yahoo.co.in

Abstract

In Contrast with traditional networks, ad hoc networks not require any previously built infrastructure, they are distributed and fully self-organized systems. Due to absence of any fixed node, each node acts as a router, providing routing capabilities of the MANET. In a distributed network, with out any infrastructure communicating peers have to rely on the whole network, therefore the proper security hardly can be established. This paper proposes enhancements in Preemptive DSR to provide secured route discovery. This paper evaluates integration of Secured Routing Protocol(SRP) and Secured Message Transmission(SMT) with Preemptive Dynamic Source Routing(PDSR) to get Secured PDSR(S-PDSR), which is capable of secured route discovery.

Key words: MANET, SRP, SMT, Preemptive DSR

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is an autonomous collection of mobile nodes having no centralized control or fixed infrastructure to support the network and it is entirely distributed. MANET topology is dynamic; nodes enter and leave the network continuously. Each node in the network acts as host as well as router and forwards the packets to destination node.

Due to frequent change in network topology, routing has become an essential network protocol in mobile ad hoc networking, MANET routing protocol in mobile ad hoc networking. MANET routing protocols are classified into two types:- Proactive (table-driven) and Reactive(on-demand) routing based on when and how the routes are discovered. Proactive routing protocols is consistent and up-to-date data routing information is available in each node, but in reactive the routes are discovered only when required by the source node.

In MANET, proactive protocols have higher overhead than reactive protocols due to continuous route updating. Reactive protocols may be used to get higher routing efficiency when only few nodes with high mobility have data to send. Otherwise proactive protocols may be used to get higher routing efficiency.

In this paper, new enhanced version of Preemptive DSR (S-PDSR), has been proposed which is based on the principle used in SRP for secured route discovery. The feature of basic PDSR to discover multiple routes is further exploited and it is suggested to incorporate the features of Secured Message Transmission (SMT) using multiple routes. It thus ensures data transmission in the data transmission phase of the MANET operation.[3]

II. CLASSIFICATION OF ATTACKS

Like all kinds of networks, passive attack and active attack are two kinds of attacks which can be launched against ad hoc networks. The passive attacks only intercept the message transmitted in the network without disturbing the transmission. By doing this, the attacker will be able to analyze the valuable information like network topology to perform further attacks. For example, by eavesdropping and subsequent analyses, the attacker may notice that some particular node is used much more than the others, which means it might be the 'heart' of this network. If this node is brought down, the whole network will be out of action as well. Then the attacker can deploy some special attacks to achieve this goal. Unfortunately, this kind of attack in wireless network is impossible to detect due to the nature of wireless network that its medium is air which is widely open to every user within the domain. The active attacks are carried out by malicious nodes which aim to disrupt transmission among other nodes or selfish nodes which may just want to save their own battery. There are mainly three ways to perform such an attack.[5]

Attacks using modification

Below we briefly talk about several modification attacks against AODV and DSR.

(1) Redirection by Modified Route Sequence Numbers:

Protocols such as AODV assign some value to routes to the specific destination to decide the priority. A route with a higher value is preferred. The node may change traffic through itself by advertising a route to a node with a greater value.

(2) Redirection with Modified Hop Counts:

Without other metrics, AODV uses the hop count field to determine a shortest path. Malicious nodes can reset

the hop count field of the RREQ to zero so that increases the chance that they are included on a newly created route. Similarly, malicious nodes may be not included in the created routes if they set the hop count field of the RREQ to infinity.

(3) Denial-of-service with Modified Source Routes:

DSR uses source routes stating routes in data packets. These routes lack integrity checks. So denial-of-service attack can be launched by altering the source routes in packet headers so that the packet can not be delivered to the destination.

Attacks using Fabrication

When a node misrepresent the identity in the network such as by altering MAC or IP address in outgoing packets, spoofing can occur. It can modify the rooting of some nodes then lead to loops in the network which will increase the power consumption greatly.

Attacks using Impersonation

These attacks generate false routing messages which can be difficult to distinguish from invalid constructs.

(1) Falsifying Route Errors in AODV and DSR:

In ADOV and DSR, if the destination node or an intermediate node along the active path moves, the node upstream of the link break broadcasts a route error message to all active up stream neighbors. This message causes the corresponding route to be invalid. A denial-of-service attack can be achieved by sending route error messages indicating a broken link on the route, then prevent the source from communicating with destination.

(2) Route Cache Poisoning in DSR:

A node overhearing may add the routing information contained in the packet's header to its own route cache. An attacker can exploit this method of learning modify route caches by transmitting packets containing invalid routes in their headers.

III. OVERVIEW OF PREEMPTIVE DSR

Assumptions:

We assume that all nodes wishing to communicate with other nodes within the ad hoc network are willing to participate fully in the protocols of the network. Each node participating in the network should also be willing to forward packets for other nodes in the network.

We refer to the minimum number of hops necessary for a packet to reach from source to destination. We assume that he diameter of an ad-hoc network will be small(5 to 10 hops), but greater than 1. Packets may be lost or corrupted in transmission on the ad-hoc wireless network. A node receiving a corrupted packet can detect the error and discard the packet.

Nodes within the ad hoc network may move at any time without notice, and may even move continuously, but we assume that the speed with which nodes move is moderate with respect to the packet transmission latency and wireless transmission range of that particular network hardware in use. Preemptive DSR can support very rapid rates mobility, but we assume that nodes do not continuously move with high peed, because it may flood data packet in ad-hoc wireless networks. The wireless communications link between each pair of nodes will be bi-directional. But some time the wireless link between two nodes may be uni-directional also.[2]

The Algorithm:

a) Route Discovery:

Step 1: When a source node S wants to send a data, it broadcast the RREQ packet to its neighbor nodes.

Step 2: When an intermediate node on the route to the destination receives the RREQ packet, it appends its address to the route record in RREQ and re-broadcast the RREQ.

Step 3: When the destination node D receives the first RREQ packet, it starts a timer and collects RREQ packets from its neighbors until quantum q time expires.

Step 4: The destination node D finds the two (primary +Backup) best routes from the collected paths (Step 3) within the quantum q time.

Step 5: The destination node D sends RREP packet to the source node S by reversing (RREQ) packets which includes the two routes (Primary +Backup) for further communication.

b) Route Monitoring:

Step 1: Each intermediate node on the route starts monitoring the signal strength.

Step 2: If signal strength falls below the specified threshold T, it will send a warning message “Path likely to be disconnected”, to the source node S.

c) The Source node S Communicates with destination node D:

Step 1: The source node S starts Communicating with destination node D using primary path.

Step 2: On receiving the warning message from the

intermediate node, it starts communicating destination node D with the backup route also.

Step 3: If source node S receives the acknowledgement form the destination node D go to step 4 else step 5.

Step 4: Preemption, switch over from Primary to Backup route.

Step 5: Initiates Route Discovery Process.

Ex:

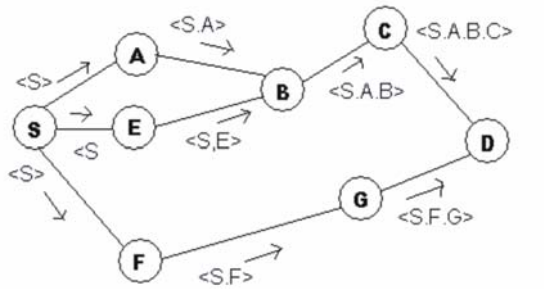

Fig. 1.

When a source node S want to send message to the destination node D, it initiates route discovery by broadcasting the RREQ packet to its neighbors (A, E, F) as shown in Fig 1. The intermediate nodes (A, E, F) on receive the RREQ packet rebroadcast the packet to its neighbors by appending its id in the route record of the RREQ packet. Similarly other intermediate nodes also forward the RREQ packet to the destination. When the destination node D receives two or more RREQ packets from the same source through different routes, it finds the two best routes based on the no of hopes. The route which has least number of hopes. The route which has least number of hops it becomes primary<S, F, G>, and second least number of hops route becomes backup route<S, A, B, C>.

The destination node D sends Route Reply (RREP) packet using the Primary (<S, F, G>) and Backup(<S, A, B, C>) route as shown in Fig. 2. Each RREP packet contains the Primary as well as the Backup route information. When source node S receives first RREP packet form destination, it treats this is the primary route and wireless communication is more error prone compared to wired network. To improve the reliability we are sending route reply (primary + backup routes information) through the primary and the secondary route. If any one packet gets corrupted at the time of transmission, source must be able to use the other packet.

IV. SECURED ROUTING PROTOCOL (SRP)

SRP works as an extension of basis protocols and ensures secured route discovery in presence of adversarial nodes, which may prevent discovery of new routes by the basis protocols. SRP introduces a set of new features which can be incorporated in Preemptive DSR(PDSR) with very low overhead. The features like, control of the query propagation, the rate of query generation etc. are all retained by PDSR. SRP only extends the basis protocol by enforcing rules on the processing of the Route Request, Route Reply and the Route Error messages, by introducing the required additional functionality for authentication.[4]

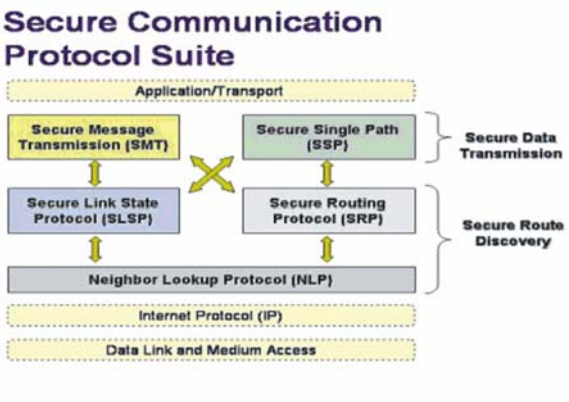

Fig. 2. SRP

SRP is based on SA (Security Association) between the Source (S) and Destination (D), which is instantiated by using public key of the other communicating end and the two nodes can negotiate a shared secret key KS, D. The basic attempt is to ensure that the packet received from a node is actually from the node which it claims to be - meaning the received packet is authenticated against the sender's id. MAC (Message Authentication Code) is calculated by using a random query identifier, query sequence number, source address, destination address and KS,D as inputs. The source S initiates the Route Discovery and constructs a Route Request packet. The Route Request packet is identified by two identifiers, which are the query sequence number and a random query identifier. The node identities (IP addresses) of the traversed nodes are accumulated in the Route Request packet. For the same example of ad hoc network, as depicted in Figure 1, the query request will be denoted by:

{QS,D;S,F,G},

where QS,D denotes the SRP header, which typically contains the query identifier, query sequence number and MAC. The type field of header is set to request. S,F and G are the ids of the intermediate nodes accumulated in the route request packet. The Route Request will traverse through the network and will reach the destination, D. The destination will construct the route replies. It calculates an MAC covering the route reply contents and returns the

packet to Source S over the reverse of the route accumulated in the respective request packet. The Route Reply will be denoted by:

{RS,D;G,F,S},

where RS,D denotes the SRP header with the type field of the header set to reply. G,F,S is the reversed sequence of the ids of the intermediate nodes used for traversing the path by the Route Reply packet. Since the destination responds to multiple requests for the same query, it provides the source with a diverse topology view. The source node S - the querying node -verifies each of the replies and updates its topology view. The topology view is maintained as per the basis protocol, which in following discussion is going to be PDSR. SMT presumes that there exists a protocol to discover the routes. For our discussion, it is presumed that the responsibility of route discovery is entrusted to SRP, with its integration with DSR as discussed in the following section.

V. SECURE MESSAGE TRANSMISSION

The goal of SMT is to ensure secure data forwarding after discovery of the route between the source and the destination, which may or may not be free of malicious nodes. It is important to understand here that SMT is a protocol which tolerates the existence of malicious nodes. SMT combines four important elements; end-to-end secure and robust feedback mechanism, dispersion of the transmitted data, simultaneous usage of multiple paths, and adaptation to the network changing conditions. SMT requires Security Association (SA) between the two communicating nodes, but does not depend on any cryptographic operations at the intermediate nodes. Active Path Set (APS) with disjoint nodes is made available at the source for use by SMT. The source disperses outgoing message into a number of pieces (P packets) at the source .Redundancy is introduced and message is encoded. At the destination, the dispersed message is successfully reconstructed to form original message, provided that sufficient number of pieces are received. Since the fragmentation of the packets is done at the source using a secret sharing technique such that if Q out of P such packets are received, the message can be reconstructed. Each dispersed piece is transmitted through a different route and each piece carries the MAC. MAC is used at the destination to verify the integrity and authenticity of its origin. The destination acknowledges the receipts of the pieces. The feedback mechanism is also made secured and fault tolerant, the acknowledgements are cryptographically protected and are also dispersed.

VI. INTEGRATION OF SRP WITH PREEMPTIVE DSR

We shall now focus on the integration of SRP with PDSR to get S-PDSR for Secured Route Discovery. There exists no security association in the PDSR protocol and it is presumed that among the nodes participating in the network none are having malicious intent. As has been discussed in the previous section, SRP can work over and above basic protocols, which now in our discussion is limited to PDSR. The source S, trying to find a route to destination D, will trigger a route discovery if there is no route available in the route cache of the source node. SRP needs a SA between the two communicating nodes and it uses two identities, for it, random request identifier and request id. MAC is calculated based on these ids and KS,D where KS,D is shared key between source and destination. It may be noted here that PDSR also needs a random id for its operation and it also accumulates ids of traversed nodes in the route request packet. In S-PDSR it is proposed to integrate the PDSR and SRP functionality into a single protocol.

The route request packet format for S-PDSR will be:

{S,D,requestid, randomrequestidentifier, MAC,NodeList : S},

only the relevant components, which are applicable for the S-PDSR are listed in the above format. As the Route Request packet will flow, ids of the intermediate nodes will get accumulated in the “Node List” of the request packet. At the end typically, it will look like the following for the example schematic of Figure 2:

{S,D,requestid, randomrequestidentifier, MAC,NodeList : S,S,F,G}.

When destination node D will receive this packet, it will first verify the authenticity of the packet, by calculating the MAC using KS,D, the secret shared key. The reply packet will flow back to the source from the destination and it will be re-verified at the source first by the SRP methodology and then by the PDSR protocol. Successful verification will cache the discovered routes in the route cache. In this process multiple routes will be discovered, since PDSR and SRP do not prevent discovery of multiple routes. Thus S-PDSR retains the basic route discovery functionality of PDSR and integrates the security aspects based on SRP proposals into its basic functioning. The secured route discovery of multiple routes between two communicating nodes is achieved in S-PDSR with minimum modifications in the methodology of PDSR and SRP.

VII. INTEGRATION OF SMT WITH PREEMPTIVE DSR

PDSR, by its design, suggests to use alternate cached routes only when the 'in use' link is broken. An alternate link from the route cache is used for continuing the data transmission. As an enhancement to the ad hoc network operations, it is now proposed to use multiple routes concurrently for data transmission, as per the

methodology suggested in SMT. It may be noted here that PDSR is only for route discovery and not for data transmission, although route maintenance is a part of the PDSR operation. The data transmission phase of the ad hoc routing protocol uses the links discovered by the route discovery phase of the protocol. SMT is one such secured protocol suggested for data transmission phase of the MANET operations. SMT strongly relies on usage of multiple routes between the communicating nodes. Data packets to be transmitted from the source to the destination are dispersed into multiple packets (P) and are routed through multiple routes simultaneously. At the destination, receipt of Q out of P packets can ensure reconstruction of the original packet.[3]

Table 1. Parameter comparison of on demand routing

Feature	DSR	Preemptive S-PDSR
Discovery of multiple paths	Yes	Yes
Secured Route Discovery	No	Yes
Advanced recovery from link breakdowns	No	Yes

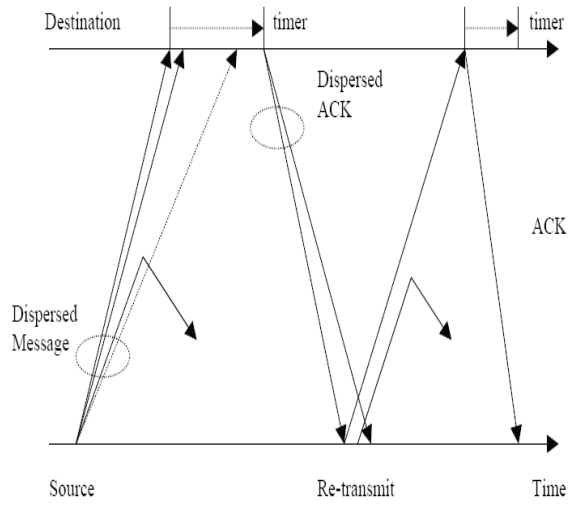

Fig. 3. Example of SMT

Figure 3 depicts how dispersed packets and acknowledgement flow takes place in SMT. Let us say for example, the data packet is dispersed into four parts (P =4) and each dispersed piece is transmitted through different routes and carries a Message Authentication Code (MAC), based on which the destination can verify the integrity of the packet and authenticity of its origin. Three out of four packets are enough to reconstruct the original message. Each packet received at the destination is acknowledged through a feedback. The feedback mechanism is also fault tolerant, secure, dispersed and cryptographically protected. In the example of Figure 4, two packets are received at the destination and two are either lost or compromised. The destination extracts information from first received packet and waits for remaining packets while setting a reception timer. On expiry of the timer, the receiver generates acknowledgement for the two successfully received packets. The sender rejects the two failing routes, on receipt of the acknowledgement packets and retransmits the two packets. One of the retransmitted packet is again compromised. Since only three out of four packets are enough to reconstruct the message at the destination, the receiver acknowledges successful reception, even before expiration of timer. This paper strongly suggests another aspect of multiple route usage. In addition to security, as dealt in SMT, S-PDSR proposes to use multiple paths for improved throughput. This multiple path usage is another feature for improved QoS for MANET operations. Integration of SMT into PDSR, giving one of the proposed extensions of PDSR results in S-PDSR that can be summarized in Table 1.

VIII. PERFORMANCE IMPLICATIONS FOR S-PDSR

Since the nodes in ad hoc network are operating under constrained conditions owing to limited battery life, limited transmission range, limited bandwidth and limited computing resource, it is essential that any protocol change/enhancement must be verified and validated for their influence/implications on the performance of the protocol. This section discusses the various related over heads, based on the enhancements suggested in the previous sections of this paper[1].

A. Proactive Route Discovery Overhead

By design, proactive protocols are not aimed at initiating route discovery unless there is a need for a route between two nodes. However in S-PDSR, it is proposed to include proactive route discovery in case number of standby routes fall below a threshold level. The associated overhead is justified, in view of the QoS factor to support continued service for applications like voice over IP, video conferencing etc.

B. Overhead of Checking Route up Status Periodically

The route status in S-PDSR is proposed to be checked periodically. Since the stand by routes are likely to be used whenever needed, their availability must be ascertained by the protocol. S-PDSR proposes to have a light weight heart beat algorithm built into the protocol. This should be triggered whenever the source is actively using the cached routes for a particular destination. S-PDSR is also proposed to have an algorithm for arranging the

cached routes for efficient selection. A suitable data structure is proposed to be worked out for organizing the cached routes at the nodes and operate using an efficient search criteria.

C. Packet Dispersion and Reconstruction Overhead

The proposed inclusion of SMT functionality in S-PDSR will disperse data into multiple packets and reconstruct the packets at the destination. This will increase the processing overheads, but will provide secured data transmission. In addition, use of multiple routes concurrently will provide enhanced throughput. For bandwidth hungry applications, use of multiple routes will improve QoS for data transmission.

D. Overhead for Basic DSR Functioning with SRP Enhancement in S-PDSR

By definition PDSR has a large route request packet and inclusion of another id and MAC will further increase the packet size in S-PDSR. This overhead due to extended packet size is marginal as compared to the size of the PDSR packet. To further compensate for this increased size, it is proposed to have a single header, instead of two (PDSR+ SRP) and achieve the required functionality of secured route discovery. Although, the processing time for the packet at each node will increase, as the computing power is increasing, it is likely to become null and void in future.

IX. CONCLUSION

PDSR is a very matured protocol and a lot of research work has verified its functioning and effectiveness. The latest IETF draft on DSR does not include the security aspects and it has been left as future work for possible enhancements. In this paper, possible enhancements to PDSR to provide security features have been proposed. Further, proposals are also made for better route cache maintenance and management. By incorporating the functioning of SRP into PDSR, new secured protocol, which has been named as S-PDSR is proposed. Concurrent use of multiple paths, as per the functioning guidelines of SMT, has further enhanced the capabilities of PDSR for secured delivery of data packets, even in presence of malicious nodes.

REFERENCES

[1]. Anil Rawat, Prakash Dttatraya and Ashwani kumar Ramani " Enhanced DSR For ANET With improved QoS", International journal of network security, Vol 5, No.2, PP.158-166, Sept 2007.

[2]. Mr. V.Ramesh, Dr.P. Subbaiah " Preemptive DSR for MANET" in InternationalConference Proceedings (ICETCSE-2008), VR Siddartha Engg. College, Vijayawada.

[3]. P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile Ad hocNetworks", Elsevier Ad Hoc Networks Journal, vol. 1, no. 1, pp. 193-209, July 2003.

[4]. Y. C. Hu and D. B. Johnson, "Securing quality-of-service route discovery in on-demand routing for Ad hoc networks", in Security of Ad Hoc and Sensor Networks 2004(SASN 2004), Washington, USA, Oct.2004.

[5]. Y. C. Hu and A. Perrig, "A survey of secure wireless Ad hoc routing", IEEE Security & Privacy, vol. 2, no. 3, IEEE Computer Society, pp. 28-39, May-June 2004.

V. Ramesh, Associate Professor, Department of CSE at MLEC, Prakasam, AP. He has published several papers in various International & National Conferences and authored the book titled "Principles of Operating Systems", Laxmi Publications, New Delhi. Presently he is pursuing his Ph. D in the field of Ad-hoc networks at Sathyabama University. His research interests include Operating Systems, Computer Networks and Data Mining.