Enhanced DSR for MANET with Improved Secured Route Discovery and QoS

Anil Rawat[1], Prakash Dattatraya Vyavahare[2], and Ashwani Kumar Ramani[3]
(Corresponding author: Anil Rawat)
Head, Computer Centre, Centre for Advanced Technology, Indore, 452013, India[1]
Email: rawat@cat.ernet.in
Department of Electronics and Telecommunication Engineering, Shri G. S. Institute of Technology and Science, India[2]
School of Computer Science, DAVV, Khandwa Road Campus, India[3]

(Received Oct. 06, 2005; revised and accepted Dec. 10, 2005 & Feb. 6, 2006)

Abstract

Mobile Ad hoc NETwork (MANET) comprises of nodes, which are free to move randomly, yet cooperate to forward packets between source and destination over a multi-hop wireless network. Due to absence of any fixed node, each node acts as a router, providing routing capability for the MANET. Various protocols for discovery of routes between any two MANET nodes have been designed. These protocols are broadly categorized as on-demand protocols and table driven protocols. Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (AODV) are the two most matured on-demand routing protocols, while Optimized Link State Routing Protocol (OLSR) and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) are the two most matured table driven routing protocols. This paper proposes enhancements in DSR to provide secured route discovery and improved QoS. The paper evaluates integration of Secured Routing Protocol (SRP) and Secured Message Transmission (SMT) with DSR to get Secured Dynamic Source Routing (S-DSR), which is capable of secured route discovery. The proposed extension also incorporates concurrent usage of multiple cached routes for improved throughput and explores possible enrichment to route cache management resulting in improved efficiency. A novel idea of proactive route discovery, particularly for high and sustained bandwidth dependent applications like video conference, voice over IP etc., has been proposed. The paper finally concludes with remarks on a possible comprehensive S-DSR protocol, incorporating better route cache maintenance scheme, proactive route discovery and integration of SRP/SMT features for secured route discovery and secured data transmission.

Keywords: Ad hoc networks, routing protocols, security, S-DSR

1 Introduction

Mobile Ad hoc NETworks (MANET), are characterized by wireless nodes, which are free to move arbitrarily, but cooperate to forward packets for each other in a totally wireless environment [2]. The routing requirement of a mobile ad hoc network is achieved in distributed fashion among the nodes. Various route discovery protocols have been designed for mobile ad hoc networks. Like other multi-hop networks, there are two phases of MANET operations: the route discovery phase and data transmission phase. Routing protocols are responsible for the route discovery phase. However, since the data transmission phase solely depends on paths discovered in the route discovery phase, it is imperative to look into the data transmission phase as a logical next step of route discovery.

The routing protocols are categorized into two broad categories: namely, on-demand protocols and table driven protocols. They are also known as reactive and proactive protocols respectively. Dynamic Source Routing (DSR) [6] and Ad hoc On Demand Vector (AODV) [10] routing protocol are two most matured on-demand routing protocols, while Optimized Link State Routing Protocol (OLSR) [1] and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [7] are the two most matured table driven routing protocols. These protocols have emerged from discussions in the Internet Engineering Task Force (IETF), the principal protocol standards development organization for the Internet.

Both the protocols are based on a similar philosophy of flooding the network with route requests and finding a route from source to destination by forwarding the route request packet from node to node, in broadcast mode. Necessary provisions have been made in the protocol functioning to ensure assured and loop free discovery of a route between the two nodes desiring to communicate in ad hoc network.

Figure 1 shows logical view of a typical ad hoc network,

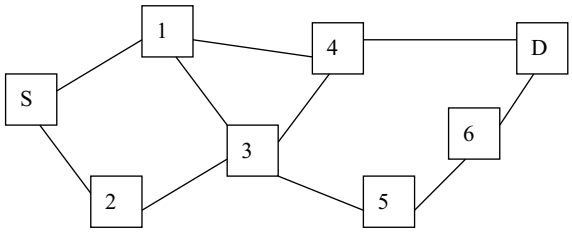

Figure 1: Typical logical Ad hoc network schematic

where, S denotes the source and D denotes the destination. Nodes 1 to 6 are the other intermediate nodes in the network and the links connecting them as shown in the figure are instant logical links, which depend on the transmission range of the nodes. As is evident from the figure, multiple paths between S and D are possible and they are S-1-4-D, S-1-3-4-D, S-1-3-5-6-D, S-2-3-5-6-D, S-2-3-4-D and S-2-3-1-4-D. The selection of a path from the given choices depends on many parameters, which includes minimum acceptable latency, maximum available bandwidth etc.

AODV and DSR are based on the fact that all nodes in the ad hoc network are willing to forward packets for other nodes and there are no malicious nodes in the network. Although, this fact cannot be taken as a very valid presumption, particularly when applications in Defense are envisaged for the ad hoc networks, in which case malicious nodes may exist. No comprehensive model for security assessment has been reported till date, which can be verified using formal methods. Attempts have been made to explore possibility of securing the route discovery and in one such attempt, Secured Routing Protocol (SRP) [9] has been proposed. This protocol is based on a Security Association between the two communicating nodes.

In this paper, new enhanced version of DSR, called as Secured DSR (S-DSR), has been proposed which is based on the principal used in SRP for secured route discovery. The feature of basic DSR to discover multiple routes is further exploited and it is suggested to incorporate the features of Secured Message Transmission (SMT) [8] using multiple routes. It thus ensures secure data transmission in the data transmission phase of the MANET operation.

Quality of Service (QoS) is another aspect discussed in this paper. It is proposed to enhance usage of route cache generated by DSR to improve QoS for MANET operations during the data transmission phase. The route cache is proposed to be divided into two segments, each containing a list of 'live' routes and 'stand by' routes. A proactive route discovery is proposed in S-DSR to discover routes whenever the 'stand by' route cache number falls below a minimum threshold level as set by the source node. Concurrent use of multiple paths for load sharing and increased throughput are, therefore, automatically achieved when the SMT features are used for data transmission in ad hoc network.

In Section 2 details of DSR functioning has been explained and in Section 3 SRP/SMT features have been discussed. Section 4 discusses proposed enhancements of DSR for secured route discovery and Section 5 is on proposed enhancements using multiple routes in S-DSR. Route caching enhancements are discussed in Section 6 and Section 7 discusses the performance implications for S-DSR. The paper concludes in Section 8 with analytical study of performance of the enhancements in S-DSR.

The paper is based on well researched studies of the latest changes made and proposed in the DSR protocol, which is still in a IETF draft stage and its simulations are still being worked out. There is a great scope to balance performance against security in ad hoc routing protocols and the same has been analyzed and evaluated in this paper.

2 DSR Protocol Details

Section 2.1 describes the basic functionality of DSR and in the next sub-section the parameters for QoS have been discussed.

2.1 DSR Functioning

Dynamic Source Routing protocol gets its name from the concept of source route, where the source node - S - includes list of all intermediate nodes (through which the packet would traverse) in the packet itself, whenever it desires to send the packet to a destination node - D - in an ad hoc network. In case there is no route available in the cache, S initiates a Route Discovery procedure. Each route discovery may discover multiple routes and all routes are cached at the source node.

Consider for example route request packet flow in DSR as shown in Figure 2, where the initiator (source S) desires to find a route to the target or the destination D.

The source S assigns a unique request id (id = 8, in the above example) and broadcasts the packet, which is received by node N1 and in turn it is re-broadcasted by node N1, after appending its own identity to the node list. The process goes on, till the packet is received by the destination - D, which in the above case will accumulate the ids N1, N2, N3 and N4 of intermediate nodes.

Since the destination may receive multiple packets from different routes for the same request id, the destination replies back to all the received packets. The Route Reply packet is sent back by the destination to the source by reversing the received node list accumulated in the Route Request packet. The reversed node list forms the 'Source Route' for the Route Reply packet. Figure 3 depicts a typical Route Reply packet from destination to the source, where NS represents the Source Route list, in the present example it will be N4, N3, N2, N1, which is the list of all the intermediate nodes traversed by the route request packet. Thus, D actually represents the source for the Route Reply packet.

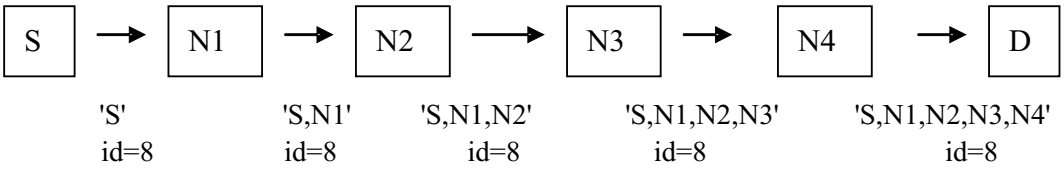

Figure 2: Route request packet flow in DSR

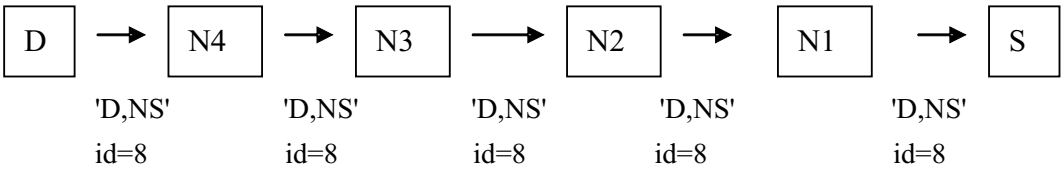

Figure 3: Route Reply packet flow in DSR

Typically, as shown in Figure 1, an intermediate node may not receive an acknowledgement from a neighboring node, triggering a Route Error packet to flow back to the source, informing Source and also all intermediate nodes of the link failure. In such a case all nodes, including source, will remove the route entry from their respective route cache. For example, Node 3 may not get an acknowledgement from Node 4, thus representing a route breakdown from S to D. In such a case Node 3 will notice the failure first and it will inform the source about the link failure.

Above description is a very broad description of the DSR protocol functioning. Many enhancements are incorporated in the DSR which are described in [6]. However, basic functioning of DSR is sufficient to understand the proposed extensions and enhancements described in the following sections.

2.2 Parameters for QoS in DSR

In an earlier draft version 3.0 of DSR submitted to IETF, QoS Guided Route Discovery was proposed by Maltz, which was later dropped. In a paper [3] the authors have proposed to revive the earlier proposal and have analyzed possible enhancements to existing DSR for secured and QoS guided route discovery. The authors have considered three main QoS metrics, namely bandwidth, latency and jitter, for finding better routes.

QoS Guided Route Discovery allows a node to specify a QoS metrics which must be satisfied in the discovered path. It is also possible that a source may use a route which is already known from its cache. In such a case, route discovery can still be performed to find a better route.

In QoS Guided Route Discovery a node sending a Route Request packet inserts in the request an optional QoS Request Header. The QoS Request Header indicates the type of resource, the minimum acceptable resource level, and the resource level of the current path. Based on these values the node receiving the request packet can decide if it can support a flow with resources at a level which are at least equal to the minimum requested.

The QoS Request Header in a Route Request only determine if the requested resources are available along the path, limiting the Route Discovery to return only paths that meet at least the minimum level of resources requested. An intermediate node that propagates a Route Request containing QoS Request Header may also temporarily reserve the resources specified in the Request in order to improve the likelihood that the resources will still be available when data flow begins using this route.

The author of [3] also proposes a mechanism for route authentication between the source and destination. The author has proposed a SQoS protocol for secured route discovery with QoS support and the methodology is based on hash chain symmetric cryptography.

3 SRP/SMT Suit of Protocols

DSR and AODV are based on a presumption that all nodes participating in ad hoc network do so in good faith and without malicious intent to corrupt the routing ability of the network. This may not be a valid assumption in case of certain category of applications (particularly Defense). Therefore, it has been felt that security is a major concern for routing protocols for ad hoc networks [4]. Many attempts have been made to secure these protocols for example Secured AODV (SAODV) [12] has been proposed as an extension of AODV. Ariadne [5] and SRP are more generic type of secured protocol extensions.

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. SMT (Secured Message Transmission) of the SRP/SMT protocol suit is for secured data transmission and is based on reconstruction of the original data

packet from multiple fragmented packets received through different routes.

SRP introduces a set of new features which can be incorporated in DSR with very low overhead. The features like, control of the query propagation, the rate of query generation etc. are all retained by DSR. 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.

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 [13]. 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 2, the query request will be denoted by:

$$\{Q_{S,D}; N1, N2, N3, N4\},$$

where $Q_{S,D}$ denotes the SRP header, which typically contains the query identifier, query sequence number and MAC. The type field of header is set to request. N1, N2, N3 and N4 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:

$$\{R_{S,D}; N4, N3, N2, N1\},$$

where $R_{S,D}$ denotes the SRP header with the type field of the header set to reply. N4, N3, N2, N1 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 DSR.

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. 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.

4 Enhancement of DSR for Secured Route Discovery

We shall now focus on the integration of SRP with DSR to get S-DSR for Secured Route Discovery. There exists no security association in the DSR 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 DSR. 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 $K_{S,D}$ where $K_{S,D}$ is shared key between source and destination. It may be noted here that DSR also needs a random id for its operation and it also accumulates ids of traversed nodes in the route request packet. In S-DSR it is proposed to integrate the DSR and SRP functionality into a single protocol.

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

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

only the relevant components, which are applicable for the S-DSR 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:

$$\{S, D, requestid, randomrequestidentifier, MAC, NodeList : S, N1, N2, N3, N4\}.$$

When destination node D will receive this packet, it will first verify the authenticity of the packet, by calculating the MAC using $K_{S,D}$, 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 DSR protocol. Successful verification will cache the discovered routes in the route cache. In this process multiple routes will be discovered, since DSR and SRP do not prevent discovery of multiple routes.

Thus S-DSR retains the basic route discovery functionality of DSR 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-DSR with minimum modifications in the methodology of DSR and SRP.

5 Enhancements Using Multiple Routes

DSR, 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 DSR is only for route discovery and not for data transmission, although route maintenance is a part of the DSR operation.

Thus, DSR does have provision to re-initiate route discovery whenever the route is lost and it maintains multiple routes in the route cache at the nodes. 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 [8].

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.

Table 1: Parameter comparison of on demand routing protocols

Feature	AODV	DSR	S-DSR
Discovery of multiple paths	No	Yes	Yes
Concurrent use of multiple paths	N.A.	No	Yes
Secured route discovery	No	No	Yes
Proactive / advanced recovery from link breakdowns	No	No	Yes

Figure 4 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-DSR 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 DSR, giving one of the proposed extensions of DSR results in S-DSR that can be summarized in Table 1.

In Table 1 AODV has been included for the completeness of the proactive routing protocols for mobile ad hoc networks. AODV does not support multiple routes in any way, nor it has any provision for discovery of multiple routes [11].

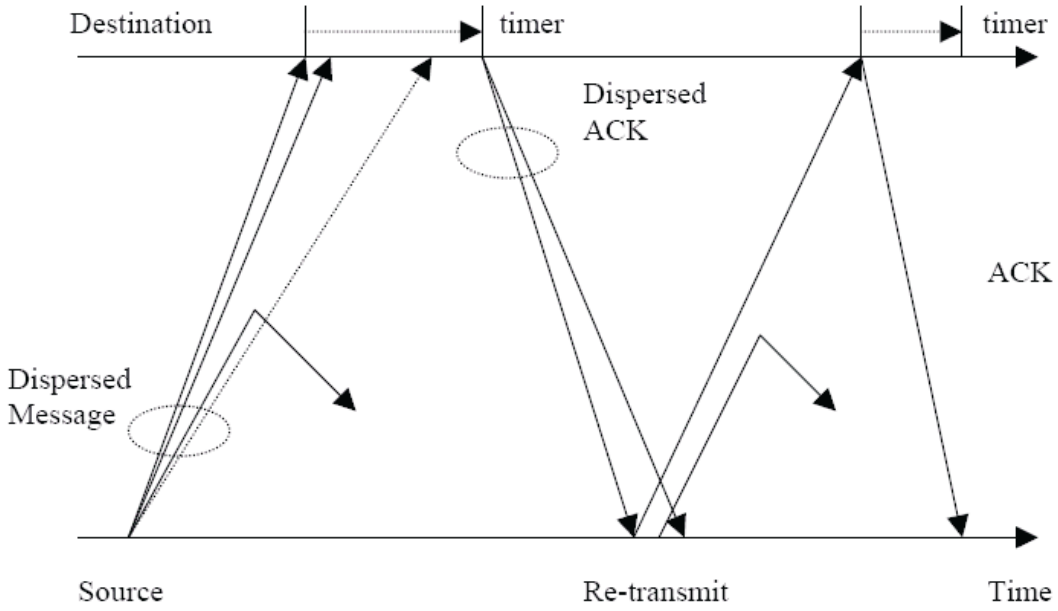

Figure 4: Sample example of SMT protocol [8]

6 Enhancement of DSR Route Caching

DSR discovers multiple routes between two communicating nodes and these routes are cached at the end nodes, as well as on the intermediate nodes. DSR also suggests techniques to improve the cache contents. The most practical are, by supporting techniques based on caching overheard routing information and by replying to route requests using cached routes. However as far as usage of multiple routes cached at the node is concerned, DSR is silent, except for using an alternate route in case of link failure.

In this section an augmented approach to cache management is proposed. Four major enhancements proposed are as follows.

6.1 'live' and 'stand by' Routes

Cached routes are to be categorized as 'live' and 'stand by'. Number of 'live' routes may be multiple. It may be recalled that SRP extends DSR capability in a secured fashion and thus S-DSR is capable of discovering multiple secured routes between the source and the destination. Multiple routes in the cache other than 'live' are also designated as 'stand by'.

6.2 Route Selection Based on QoS Metrics from the Cache

QoS metric for the DSR protocol as proposed by Hu [3] is based on three primary parameters. These parameters are: bandwidth, latency and jitters. In S-DSR it is proposed to define the selection criteria for the routes from the cache which is based on these parameters. For the example in Figure 1, let us assume the link parameters between the nodes as per the Table 2.

With the above parameters a typical route cache at the source S may look like as shown in Table 3.

Minimum bandwidth is the bandwidth of the weakest link in the route. Latency and jitter are cumulative figures, as generated by all the intermediate nodes put together. Latency and jitter are computed in milliseconds (ms), while bandwidth is typically mentioned in Kbps. The time stamping is used for stamping latest route verification for availability.

For an efficient selection of route from the cache, the routes may be sorted on a periodic basis and the sorting criteria could be defined by the source, based on the application's need. The best cached route will top the list for efficient selection by the S-DSR algorithm. Data structure for efficient route search is being worked out.

6.3 Proactive Route Discovery for Uninterrupted/Continued Operation

As long as routes are available in the cache, DSR is able to sustain continued support for data transmission. In case there are no routes available in the cache, and the one which is being used is broken, DSR re-initiates route discovery. This may not be an acceptable mode of operation, particularly for applications, which are dependent on bandwidth and need ensured uninterrupted connectivity.

When the application demands that a route is available for data transmission without any disruptions, this proposed concept of proactive route discovery enhances the required QoS parameter of route reliability to a great extent. S-DSR includes proactive route discovery, which is

Table 2: Link parameter between various nodes of Figure 2

Link	Bandwidth, latency, jitter (Kbps, ms, ms)	Link	Bandwidth, latency, jitter (Kbps, ms, ms)
S-1	128, 10, 8	S-2	128, 16, 1
1-4	128, 14, 2	1-3	64, 12, 7
2-3	64, 16, 2	3-4	128, 13, 5
3-5	512, 12, 12	5-6	512, 14, 3
4-D	128, 16, 1	6-D	64, 12, 2

Table 3: Typical route cache entries in S-DSR

Destination	Intermediate Node list	Minimum Bandwidth (Kbps)	Latency (ms)	Jitter factor (ms)	Time stamp	Category
D	1-4	128	40	11	13:40:45:75	L
D	1-3-4	64	51	21	13:40:43:00	L
D	1-3-5-6	64	60	32	13:40:43:99	S
D	2-3-5-6	64	70	20	13:41:06:23	S
D	2-3-4	64	61	9	13:41:12:45	S
D	2-3-1-4	64	74	13	13:41:13:13	S

L: Live Route
S: Standby Route
Time stamp: hour: minute: second: milliseconds

triggered when the number of standby routes falls below a threshold level.

A threshold level is set by the source for the 'stand by' routes. This threshold level will depend on the application for which the source is using the route. In case of bandwidth and throughput dependent applications, it is imperative that the continuity of data transmission is ensured. In such cases, the source will set the 'stand by' threshold value to a reasonably high number.

6.4 Proactive Validation of Cached Routes

Cached routes are used by DSR and also by the proposed S-DSR, only when they are needed by the source. Since there is no provision in the protocol definition to proactively check the route's availability, it is suggested in S-DSR to proactively check the routes in the cache for their availability.

This feature in S-DSR is proposed to be supported by some heart beat algorithms, used for this purpose. To reduce the associated overhead of this proposed enhancement, it is suggested to incorporate only a very light weight extension of DSR to check the availability of the cached routes in the S-DSR.

7 Performance Implications for S-DSR

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 overheads, based on the enhancements suggested in the previous sections of this paper.

7.1 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-DSR, 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.

7.2 Overhead of Checking Route up Status Periodically

The route status in S-DSR 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-DSR 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-DSR 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.

7.3 Packet Dispersion and Reconstruction Overhead

The proposed inclusion of SMT functionality in S-DSR 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.

7.4 Overhead for Basic DSR Functioning with SRP Enhancement in S-DSR

By definition DSR has a large route request packet and inclusion of another id and MAC will further increase the packet size in S-DSR. This overhead due to extended packet size is marginal as compared to the size of the DSR packet. To further compensate for this increased size, it is proposed to have a single header, instead of two (DSR + 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.

8 Conclusion

DSR 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 DSR 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 DSR, new secured protocol, which has been named as S-DSR is proposed. Concurrent use of multiple paths, as per the functioning guidelines of SMT, has further enhanced the capabilities of DSR for secured delivery of data packets, even in presence of malicious nodes.

Concurrent use of multiple paths and introduction of the concept of 'live' and 'standby' routes in the cache, can provide an additional strength to S-DSR for improved QoS by enhancing the availability, throughput and reliability. Proactive route discovery, when the number of standby routes goes below a threshold level, adds a new dimension to the QoS supported by DSR.

Analytical study of various related overheads after incorporating the new features to introduce S-DSR has been discussed in the paper and implications arising out of new route cache maintenance have also been discussed. It has been found that with limited increase in the overhead a far more robust and efficient protocol named S-DSR has emerged out.

References

[1] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)", *RFC 3626 of IETF*, Oct. 2003.

[2] S. Corson and J. Macker, "Mobile Ad hoc networking (MANET) routing protocol performance issues and evaluation considerations" *Request for Comments 2501 (RFC) of Internet Engineering Task Force (IETF)*, Jan. 1999.

[3] 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.

[4] 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.

[5] Y. C. Hu, A. Perrig, and D. B. Johnson, "Aridane: A secure on-demand routing protocol for Ad hoc networks", in *Proceedings of the Eight Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pp. 12-23, Sept. 2002.

[6] D. B. Johnson, D. A. Maltz, and Y. C. Hu, "The dynamic source routing protocols for mobile Ad hoc networks", Internet-Draft, draft-ietf-manet-dsr-10.txt, Work in progress, July 2004.

[7] R. Ogier, F. Templin, and M. Lewis, "Topology dissemination based on reverse-path forwarding (TBRPF)", *RFC 3684 of IETF*, Feb. 2004.

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

[9] P. Papadimitratos, Z. J. Haas, and P. Samar, "The secure routing protocol (SRP) for Ad hoc networks", Internet-Draft, draft-secure-routing-protocol-srp-00.txt, Sept. 2002.

[10] C. E. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing", in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA*, pp. 90-100, Feb. 1999.

[11] E. Royer and C. K. Toh, "A review of current routing protocols for Ad-hoc mobile wireless networks",

IEEE Personal Communications Magazine, pp. 46-55, Apr. 1999.

[12] M. G. Zapata, "Secure Ad hoc on-demand distance vector routing for wireless networks", in *Poster presentation, ACM Symposium on Mobile Ad Hoc Networking & Computing (Mobihoc'01)*, pp. 106-107, Long Beach, California, Oct. 2001.

[13] R. Zucceratto and C. Adams, "Using elliptic curve Diffie-Hellman in the SPKM GSS-API" *Internet Draft, IETF*, Aug. 1999.

Anil Rawat received his bachelor of engineering degree in1984 from Rani Durgavati Vishvavidyalaya, Jabalpur, Inida in Electronics and Telecommunication engineering and masters in Computer Engineering from Devi Ahilya Vishvavidyalaya, Indore, India in 1991. Presently he is working at Compute Centre of Raja Ramanna Centre for Advanced Technology, Indore, India. He has published more than 30 papers in various Journals & International and National Conferences. Presently he is pursuing His PhD in the filed of Ad-hoc networks. His research interests includes computer networks, cluster and grid computing etc. His email address is: rawat@cat.ernet.in

Dr. Prakash Dattatraya Vyavahare received Ph. D. in 1994 from IIT Bombay in the field of Computer Communication and M. Tech. in Electrical Engineering (with specialization in Communication Engineering) in 1976 from IIT Bombay. He worked as a communication engineer at Tata Institute of Fundamental Research, Bombay during 1976-1982. Since 1982 he is with the Department of Electronics and Telecommunication Engineering at SGSITS Indore, where presently he is working as Professor and Head of the Department. His area of interests includes performance evaluation of computer communication network. He was Hindu-Hitachi scholar during 1981-82 at Hitachi Ltd. Japan and Rotary GSE team member to USA in 1988. He is an associate of UNESCO-ICTP Italy since 1998. He has published 15 papers in national and international journals and 17 conference papers. He has guided one Ph.D. thesis and is presently supervising 3 research scholars.

Dr. Ashwani Kumar Ramani received his Master of Engineering (Digital Systems) and Ph.D, from Devi Ahilya University (formerly University of Indore, www.dauniv.ac.in) , Indore, India in the years 1986 and 90, respectively. He worked as a research engineer in ISRO Satellite Center, Dept. of Space, Bangalore, India, during 1979-83. Later he joined the Military College of Telecommunication Engineering, Mhow, India. From 1986-89, he was assistant professor in the Department of Electronics and Computer Engineering, at S.G.S. Institute of Technology and Science , Indore, India. Since Jan. 1990, he is professor with the School of Computer Science at Devi Ahilya University. He acted as Director of International Institute of Professional Studies, Indore, India during 1993-95 and 1999-2003. He was associate professor at University Putra Malaysia, Dept. of Computer Science during May 95 to May 99. Currently, he is on one year assignment at King Faisal University (KFU), Kingdom of Saudi Arabia. Here, he is responsible as Chairman of the Accreditation Committee to pursue ABET Accreditation.