World Applied Sciences Journal 32 (6): 1130-1139, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.32.06.665

Route Maintenance Analysis in Secured Dynamic Source Routing-A Comprehensive Study

[1]S. Menaka and [2]M.K. Jayanthi

[1]School of Information Technology & Engineering, VIT University, India
[2]King Khalid University, Saudi Arabia

Abstract: Route monitoring and faster resuming of communication data transmission during link breakage in a network comprising of self organizing nodes is as important as discovering a secured route to maintain the network performance in terms of uninterrupted communication. Routing is one of the tasks in the network layer where there is more scope for an intruder to gain access to a network. Embedding security features to a routing protocol becomes necessary to thwart the malicious nodes to enter the network. The random mobility of nodes, multi-hop communications and insecure wireless environment adds to the vulnerabilities in a mobile ad hoc network that makes routing a crucial issue. Several secured routing protocols have been proposed by researchers to address the security threats to identify trustful node during the route discovery process, but the necessity of effective route maintenance to conserve the performance of routing protocols integrated with security features has not been addressed. In this study different types of secured source routing protocols, route maintenance and route cache features are discussed systematically. Further it is demonstrated to show the identified features towards the contribution on the performance of the routing protocols for securing the network from the malicious nodes.

Key words: Route cache · Route discovery · Route maintenance · Secured reactive routing protocols

INTRODUCTION

The potential of MANETs has a wide set of powerful applications including military operations, emergency rescue missions and simple provision of wireless network access, such as at a conference or in a classroom [1]. where the users can be connected to communicate at any time without any requirement of pre-deployed infrastructure. MANETs are featured by characteristics like robustness, flexibility, intrinsic mutual trust, dynamic network topology, frequent routing updates, that also adds to vulnerabilities to various security issues. One of the challenging security issues in mobile ad hoc networks is identifying a secured route to forward the data packet to a desired destination node via multi-hop nodes. The mobile nodes that are in radio range of each other can directly communicate, while the others communicate by forwarding the data packets through the intermediate nodes, which makes the node in the network to operate both as hosts and routers to communicate or forward the data packets within the network [2]. This property makes the network highly robust requiring to ensure that every node in the route of communication is trustworthy by some security mechanisms to authenticate the nodes in network that becomes a part of the route. The integrity of the messages communicated are maintained by the use of encryption techniques. The necessity of security requirements for communication between the nodes attracted various the researchers to design a secured routing protocol to authenticate the intermediate nodes and doesn't disrupt the network. Routing protocols for MANET are classified as reactive routing protocols, establishes the route only there is data packets to communicate and maintains the routes in the route cache an proactive routing protocol that maintains the routing table updated by exchange of routing information

Corresponding Aurthor: S. Menaka, School of Information Technology & Engineering VIT University, Katpadi Pin: 632 014, India. Mob: +8681034652 / 9840331632.

periodically with the current status of the topology of the network. In general [3] reactive routing protocols outperform the proactive routing due to their ability to react to topology changes quickly and reduced overhead. Reactive routing protocols consist of two phases 1) Route discovery - process of learning the route to the destination node. This phase is initiated by the node that needs to communicate referred to as the source node. The second phase is 2) Route Maintenance - Process of monitoring the active route and identifying an alternative route to the destination node when there is a change in the topology and the current route is disturbed due to the mobility of the nodes. In between these two phases the routes discovered during the route discovery phase is stored in a structure known as route cache and in the route maintenance phase the alternate routes can be selected from the route cache or request for a new one. Many secured routing protocols have been proposed to mitigate the various routing attacks in the route discovery phase to authenticate the intermediate and destination nodes. The route cache is also vulnerable to routing attacks like DDoS, route cache poisoning and so forth, similarly route maintenance phase is also vulnerable to various attacks launched by compromising nodes, which most of the secured versions of dynamic source routing protocols have not addressed at. This analysis is based on the how the route maintenance contributes towards the performance of the network. At present the security levels of all the protocols considered for study is assumed to be same with their own pros and cons of different cryptography mechanism implemented. This paper aims to compare the various secured versions of Dynamic Source Routing protocol, ARIADNE, ARAN and SRP in the perception of security of the route cache and route maintenance, highlighting the advantages and the drawbacks of the mechanisms of security provided by above mentioned protocols. The rest of the paper is organized as Section 2 briefing about DSR protocol and the route cache of DSR, section 3 discusses the secured versions of DSR highlighting the route maintenance procedure. The section 4 analyses the security characteristics of the three protocols and section 5 gives the concluding remarks.

Route Cache in Dynamic Source Routing

Overview of DSR: DSR is designed with significant features of low overhead and ability to react quickly to changing topology. The DSR protocol is highly reactive helping ensure successful delivery of data packets in spite of frequent node movement or other changes in network conditions. The DSR protocol is composed of two main mechanisms that work together to establish new routes “Route Discovery” and identify alternate/new route during link breakage “Route Maintenance”.

Route Discovery: The mechanism of the source node to find a feasible route [4] to target node is known as Route Discovery. When the source node S that wants to send a packet to a destination node D it broadcasts the Route Request (RREQ) in the network. Each ROUTE REQUEST message consists of request id, determined by the initiator of the REQUEST, the IP address of the initiator and target node identification to which the route is required [5]. The nodes that receive the RREQ packet checks if the destination address is its own address, if it's, not its address, it will record its IP address on the RREQ packet and forwards it to the next upcoming stream. When the target node receives the request packet, it unicasts a Rout Reply (RREP) packet back to the source along the same path recorded in the RREQ packet. This way the source node learns the routes available to the destination node and records in the route cache. The source node may receive multiple routes to the same destination which recorded in the cache. The source then selects the route minimum number of hops or if the number of hops is same for multiple routes, the path via which the RREP arrived first will be chosen as the primary route and the other routes will be kept as alternate routes to use in case of link breakage. Meanwhile the intermediate nodes also update its own route cache with the routes it learned during this route discovery process.

Route Maintenance: When nodes in the network move in and out of the present network range the communication breaks down. This detection of Link disturbance between the source and the destination, the source can no longer use the current route. This monitoing of link breakage and searching for a new route is known as Route maintenance [4]. When the current route to D is no more valid, source node S either tries to use any other route available to D from its route cache or initiates the route discovery again and updates its route cache with the new route to the destination D. Figure 2 depicts the Route Error message forwarded by NC to the source via NB when NG moves away from the network. Route Maintenance is done only if there is active communication between source and destination during the route disturbance.

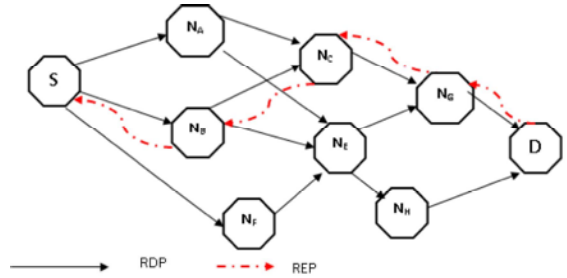

Fig. 1: Route Discovery in DSR

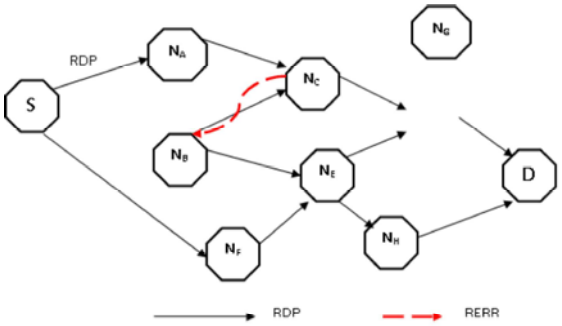

Fig. 2: Route Maintenance in DSR

$N_S \rightarrow N_B \rightarrow N_C \rightarrow N_G \rightarrow N_D$
$N_S \rightarrow N_A \rightarrow N_C \rightarrow N_G \rightarrow N_D$
$N_S \rightarrow N_B \rightarrow N_E \rightarrow N_G \rightarrow N_D$
$N_S \rightarrow N_B \rightarrow N_E \rightarrow N_H \rightarrow N_D$
$N_S \rightarrow N_F \rightarrow N_E \rightarrow N_G \rightarrow N_D$
$N_S \rightarrow N_B \rightarrow N_E \rightarrow N_H \rightarrow N_D$

Fig. 3: Path cache structure

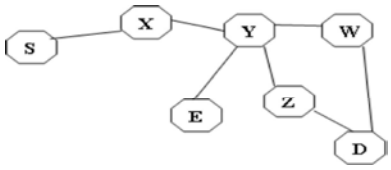

Fig. 4 : Link Cache Structure

Route Cache: Route cache is the structure in which the nodes store the learned routes for various destinations during the route discovery process. The route cache entries are useful in avoiding the route discovery process for frequently used routes [6]. There are two types of route cache, when the source caches the discovered routes is termed as source route cache and the nodes participating in the route discovery overhears the packet and records the route is called as intermediate node caching. Thus the cache will be having the current topology of the network. There are two kinds of cache structures defined, i) Path cache and ii) Link cache [3].

Path Cache: The entire path to every destinationlearned by the nodes is maintained in the route cache. The Figure 3 represents the route cache entryfor the discovered route from the source to the destination as per the current topology of the network at the source node cache as per the route discovery process shown in Figure 1. The source node will store the path as NS-NB-NC-NG-ND. In this case when there is a link break in the path as NG moves of the network, NC will inform the source as well as the other node using NG. When the source finds a new route to a destination via another NB the route cache entry will be updated with the new path as NS-NB-NE-NH-ND as in the Figure 1 and the old route to D via Y will be deleted as in Figure 2. When a link is common in routes to two destinations from the source, it will have distinct entries in route cache.

Link Cache: The route cache stores the route in conventional graph data structure by storing the links to every node. When there is a break in the link as in the above Figure 1, in the route the links Y-Z and Z-D is disconnected as Z moves from the network. The source node performs a BFS search on the cache entry and replaces only the broken link in the existing entry rather than replacing the entire path with a new entry. As shown in Figure 4, the advantage of Link cache is the common link X-Y can be shared between Z and E as stored in the cache.

Route in path cache is always present in link cache, but vice versa is not true [7]. By connecting individual links a better path can be formed, which may not be present in path cache. Whenever a link breaks a complete route in path cache is replaced while in link cache only broken link is deleted and other links remains same, as in the Fig. 4.

The major security threats for the existing Dynamic source routing protocol can be categorized as [8] Modification Attacks, Impersonation Attacks, Fabrication Attacks.

Modification Attacks: The attacker node redirects the network traffic by altering the control message fields or by forwarding falsified route message claiming that it has a feasible route to the destination. Modifications of the Route hop count, Modification of Source Route, Tunneling are some two types of modification attacks on DSR.

Impersonation Attacks: This type of attacks where the authenticity and confidentiality of a node is violated in a network. A malicious node can impersonate or spoof the address of another node and redirects the data packet towards itself rather than to destination. The attacker tries to alter the visibility of the network topology as perceived by any other legitimate node.

Fabrication Attack: The target of fabrication attacks is to drain off limited resources in other MANET nodes, [9] such as battery power and network connectivity by flooding a specific node with unnecessary routing messages. A malicious node can for example, send out false route error messages. These types of attacks are difficult to detect, where the malicious node generates false routing claiming that the intermediate node on the route cannot be reached by sending RERR packets [1]. These types of messages generated by the attacker are generally termed as fabricated route messages. Falsifying Route Errors, Route Cache Poisoning in DSR are the two common attacks in DSR under this category. Among the above mentioned attacks in DSR, Attack using Fabrication is the one that targets to attack the route cache and route maintenance process. Many secured routing protocols proposed by the researchers focus on the secured route discovery that authenticates the nodes participating in the discovery process are legitimate nodes. Hence it is assumed that the routing messages that are exchanged after route discovery phase as a valid message from legitimate users, but during the route maintenance also the attacker can gain the access to the network. A fabrication attack can also be launched by a selfish node that duplicates the transmission of packets to another node, just to make sure all packets will reach the destination node that leads to an excessively high network traffic load [9], modify the contents of route cache diverting the source or other nodes to take a path via the attacker that introduces packet drop attacks or to track any confidential communications, etc. change to a new route when the current path is active or even launch a Denial of Service attack such that the intermediate nodes are unavailable to forward the packets by continuously sending RERR message.

Secured DSR Routing Protocols: Securing of the routing attack can be achieved either by preventing the attack or detecting and recovering of the attack. [10,11] The Figure 5 below preset the taxonomy of the secured routing protocol in both aspects of prevention and detection.

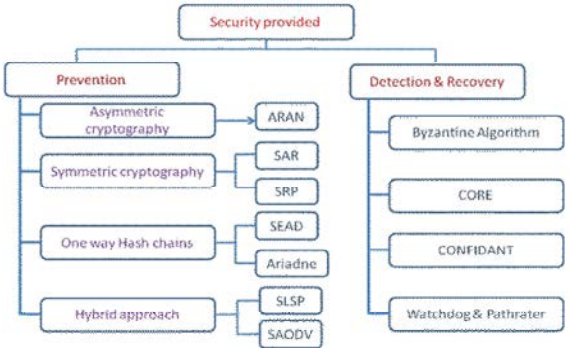

Fig. 5: Taxonomy of Secured Routing Protocols

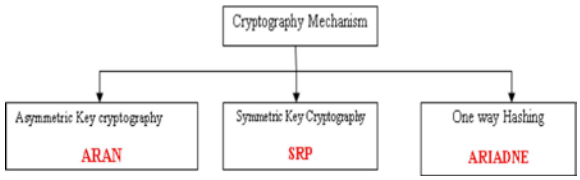

Fig. 6: Taxonomy of DSR Secured Routing Protocols

Extensive researches have proposed many secured routing protocols for MANETs, by embedding security based measures with the routing algorithms [12,13]. Some of the common secured reactive routing protocols existing are ARAN, SRP, SAR, SEAD, Ariadne, SLSP and SAODV. Among the above the secured routing protocols mentioned, ARAN, SAR, SRP, ARIADNE and SAODV are based on reactive routing protocols while SLSP and SEAD are based on proactive routing protocols. Each protocol has its own pros and cons which is used as per the application requirement of the network [14]. Considering the security provided by the existing secured routing protocols be it prevention or detection/recovery, the aspiration of any source routing protocol is to ensure the intermediate nodes are trusted nodes such that they will not add any malicious node in the path or remove any legitimate nodes from the route. Many secured versions are proposed extending the DSR embedding with security based measures [12,13]. Each algorithm has various security mechanisms to authenticate the user during the route discovery process. The Figure 6 gives a taxonomy of the DSR secured routing protocols based on the cryptographic mechanism adopted in each protocol [15].

Each protocol has its own strength and weakness in terms of algorithm complexity, immunity towards specific routing attacks as given in the Table 1. The rest of this paper further discusses the cryptography mechanisms used in the above set of protocols analyzing their performance based on the protection of the route cache and its impact on route maintenance.

ARAN - Authenticated Routing for Ad Hoc Networks: Authenticated Routing for Ad-hoc Network (ARAN) [15.] is based on asymmetric key cryptography. ARAN introduces *authentication*, *message integrity* and *nonrepudiation* to routing in an ad hoc environment as a part of a minimal security policy [15]. Every node of the network is authenticated by a cryptographic certification issued by a trusted certification authority (T) who distributes its public key to all the nodes in the network. Each node receives one certificate from T after securely authenticating its identity to T.

T_A : cert A=[IPA, KA+, t, e]KT- (1)

The certificate contents are the IP address of node S (IPS), the public key of S (KS+), timestamp (t) when the certificate was created and validity time of the certificate (e) digitally signed by the public key of the certificate authority (KT-). These certificates are revoked when they leave the network. The next step is the end-to-end authentication of route discovery that verifies whether the intended destination is reached. The source broadcasts a digitally signed Route Discovery Packet (RDP) that includes the certificate of the initiating node, a nonce, a timestamp and the address of the destination node.

S ->broadcast : [RDP, IPX, NS]KS-, certS (2)

Nonce and timestamp prevent replay attacks and to detect looping and appends its signature on the packet. All subsequent intermediate nodes, remove the signature of the previous node, verify it and append their signature on the packet [1, 15]. The destination node X receiving the RDP unicast the signed reply packet (REP) and each node appends its signature before forwarding it to the next hop termed as the authenticated route setup.

X □ D: [REP, IPX,NS]KX-, certX (3)

Route Maintenance in ARAN: An error message is generated and forwarded to the source node if the data is received from an inactive or broken node. For example node C along the current active route recognizes a broken link to the destination forwards the signed ERR message to its upstream node addressed to the source and destination. The nonce field in the ERR message indicates the freshness of the ERR message.

C_B : [RERR, IPS, IPX, NC]KC-, $cert_C$ (4)

Security Analysis of ARAN: The fabrication of the ERR messages for active link are extremely difficult to detect, but offer a deterrent, by ensuring non-repudiation and prevents impersonation that could be useful to identify the attacker and revoke the certificate and prevent the node from further communication [16]. There is danger of the attacker launching a Denial of service attack by sending signed ERR message for any active or non broken links that can cause widespread congestion and power loss to all nodes. ARAN is also vulnerable to attacks like increase measured time of the path by delaying the REP and hence conspire to elongate the routes, forcing the source and destination to pick up a route favored for the attackers. High computational cost as every certificate is cryptographically signed and verified at every node along the route and the risk of single point failure of the Trust authority adds to the demerits of ARAN.

SRP - Secure Routing Protocol: The Secure Routing Protocol was proposed by Papadimitratos *et al* [1]. is specially designed to be compatible with any of the reactive routing protocols. SRP uses symmetric key cryptography to operate based on the Route querying method [17]. SRP operation is based on establishing a Security Association (SA) between the source and destination nodes, thus authenticating the routing messages along with the communicating parties. A hybrid key distribution procedure is used to establish the SA [15]. A secret symmetric key (KS, D) is exchanged between the sender and the destination with the public keys of the each other. Source (S) and destination (D) authenticate routing messages over the secured channel by the secret symmetric key (KS, D). When SRP is implemented with DSR, it requires a 6-word header with the unique identifiers of route discovery process and message authentication code (MAC) computed using a keyed hash algorithm that is added to the base header.

As per the above Fig. 1 The route request message is denoted by :

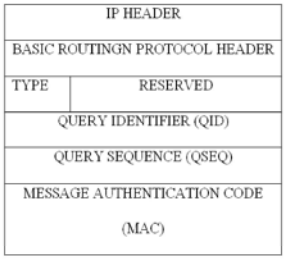

Fig. 8: SRP Header

$$\{Q_{S,D};N_A,N_B,N_F\} \quad (1)$$

The header consists of a query sequence number (QSEQ), query identifier (QID) and the output of a key hashed function. The IP header, the header of the basic routing protocols and shared key of SA are the parameters to the key hash function. The QID is used to avoid multiple entries of the path in the route cache. The destination node on receiving the RREQ checks the security metrics by computing the MAC, verifies the secret key and generated reply packet for the source node adding the fields QID, QSEQ. The Route Reply is denoted by:

$$\{RS,D; NG, NC,NB,S\} \quad (2)$$

Where RS, D denotes the SRP header with the type field of the header set to reply. The source node S - the querying node verifies each of the replies and updates its topology view.

Route Maintenance in SRP: This process is done through route error messages, 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. SRP is an extension of the basis protocol by adding additional requirements for authentication on the processing of the Route Request, Route Reply and the Route Error messages. According to Anil Rawat et. Al [2] MAC and QID though increases the packet size and the processing time for the packet at each node in SRP can be compensated by the growing size and computing power of the mobile devices in the future. By definition DSR has a large route request packet and the 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 negligible in the future.

Security Analysis of SRP: SRP is combative to bogus route reply packets authenticating the destination and the intermediate nodes. The significance of the SRP is that it wangles correct topological information about the network. [12] SRP scrapes with colluding misrelay attacks and replay, fabrication attacks. SRP does not resistive to modification attacks during the packet forwarding, for instance node list in a RREQ packet can be easily corrupted or altered by any node while forwarding the packet. SRP does not address the security issues of route maintenance that is the RERR packets are not authentic. Secure message transmission (SMT) using secret sharing techniques are deployed to ensure successful delivery of data packets.

ARIADNE: This reactive secure routing protocol as proposed by Y.Hu et. al. Strongly depends on symmetric cryptographic authentication the routing messages using any of three schemes : [18] shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures, but strongly based on TESLA key. Ariadne uses a shared secret key (KS, D) shared between source and destination and at each intermediate node is authenticated by TESLA key that authenticate the route discovery process chain, after which the RREQ packets are forwarded thus guaranteeing secured route discovery. [12, 19].

Route Maintenance in Ariadne: Route Maintenance in Ariadne is similar as to the basic DSR operation. The forwarding node on recognizing a link breakage sends a RERR message to the source node. The error message is authenticated by TESLA to defend against the unauthorized error messages from the attacker. Any node that wants to send the RERR packet buffers it until it get the reply from TESLA [18].

A ROUTE ERROR packet consists of six fields:

<ROUTE ERROR, sending address, receiving address, time interval, error MAC, recent TESLA key>.

The sending address is the address of the intermediate node encountering the error and the receiving address is the address of the node that has broken from the link identified by failure in attempts to forward. In the figure () node C after a failure of attempts to forward packets to node G, the RERR packet will be generated and forwarded by node C, the sender's address is address of C, receiving address will be the address of G and the destination address is the source of the route. The time interval is the expected TESLA time of the destination receiving the Route error message, the error MAC is the MAC of the RERR fields computed using the Route Error's TESLA's key and the recent TESLA key is

Table 1: Merits & Demerits of DSR Secured Routing Protocols

Secured Routing Protocol	Secures from	Strength	Weakness
ARAN	Modification, fabrication, impersonation	Less complexity in terms of implementation	Expensive, not immune to worm hole attack
SRP	Detect & Discard bogus replies, fabrication of routing packets	Immune to IP spoofing	Prone to Route cache poisoning, not immune to work hole attack
ARIADNE	Modification, fabrication of routing information, flooding	Immune to worm hole attack	Selfish nodes are not taken into account

set to "most recent". The forwarding nodes also authenticate and process the Route Error in the similar way.

Security Analysis of ARIADNE: The significant features of ARIADNE are providing point to point authentication using message authentication code and shared key. Ariadne uses time stamps that prevents spoofing attacks and path loops as the packets are forwarded only via authenticated legitimate nodes. The major strengths of this protocol include protection against wormhole attack and route cache poisoning attack, but it is not immune to Rushing attack, Routing table alteration, Denial of-service Attacks as well as Black hole attack.

Route Cache Analysis of Secured Dsr Routing Protocols: In a nutshell, all the above discussed secured routing protocols in general the route cache maintenance are featured as:

- ROUTE ERROR messages are processed in a similar way authenticating other route discovery messages exchanged.
- Every intermediate node generates route error message only after the failure of number of retransmission attempts to deliver the packet to broken links.
- ARAN's route error packets are vulnerable to fabrication attacks. It also involves higher computational costs at each node which accounts for energy costs and latency.
- SRP requires high clock synchronization [17] and same level of trust level to share a common secret for secure communication which is not practically feasible to achieve.
- Ariadne suffers from the infeasibility in TESLA Authentication due to requiring of predeployed keys, resulting in delay in packet delivery. In the presence of malicious node only the sender can identify the modification of reply messages according to Chu *et al* [20].

Table 2: General Parameters for simulation

Parameters	Values
Number of Nodes	50
Topology area	1000 x 1000
Traffic type	CBR (Constant Bit Ratio)
Mobility Model	Radom Way Point model
Simulation Time	600 secs
Source Destination pairs	5
Application Data Payload	512 bytes / packet
No: of packets	4 packets/second
Physical Link Bandwidth	1 Mbps
Cache size	15 routes
Cache Replacement Policy	FIFO

Table 3 :Protocol Specific Parameters

Protocol	Parameter	Values
ARAN	RSA Key Size	512 bits
	Signature size	16 bytes
	Signature generation delay	5.5ms
	Verification delay	0.5ms
ARIADNE	TESLA Time Interval	1 second
	Hash Length	80 bits

Apart from the above mentioned features, the route cache of the secured routing protocols still suffers from the problems of inefficient management of active and deactivated routes in route cache due to lack of mechanism to update the multiple routes and fresh routes information to distinguish between broken routes and alternate routes [20].

Incomplete Error Notification, No Expiry, Quick Pollution are some the causes for stale routes in the route cache, which any of the secured DSR routing protocols have not addressed [21]. The following Table 1 summarizes the strength and weakness of the secured routing protocols. The performance of route maintenance and route cache of secured routing protocols ARAN, SRP and ARIADNE evaluated from the simulation results in NS2 using the parameters alternate route acquisition latency during the link breakage and the impact of the same on data packet loss and routing load.

Simulation and Results: The above three secured source routing protocols ARAN, SRP and ARIADNE are further

analyzed by simulating the protocols using the NS2 simulator to study the impact of route maintenance on the performance of the protocols. The simulating environment and results are discussed in the forthcoming sections.

Simulation Environment: Dynamic source Routing (DSR) is the basic routing protocol for ARAN, SRP and ARIADNE secured routing protocols. NS2 simulator is used to simulate the above algorithms for the study with the following parameters set for various protocols discussed in this paper. Table 2 lists the simulation parameters and the protocol specific parameters are given in Table 3. The entire simulation is run for 10 iterations for the analysis purpose and the results are plotted for discussion in the next section.

RESULTS AND DISCUSSION

Figures 7 to 10 show the simulated results analysis of the three DSR secured routing protocols, ARAN, SRP, ARIADNE. The analysis is based on the attributes like, Route acquisition latency, ratio of data packet loss, routing load end to end delay in transmission.

In Figure 8 it is inferred that ARIADNE has a lesser latency than ARAN and SRP. Though ARIADNE has additional propagation time with TESLA for authentication, it tradeoffs with the computational time to validate the node authentication procedures incurred in the other two protocols. Route acquisition initially is the time taken for route discovery, while the node keeps moving in and out of the network, route acquisition latency is measured as time interval between the receipt of the RERR message at the source and receipt of the data packet at the destination via the new route.

The Figure 9 shows the end to end delay in delivery of data packets interprets the response is almost similar for ARAN and ARIADNE, while it slightly more in the case of SRP. This is due to the clock synchronization requirement the processing time taken to verify and validate QID & QSEQ, while for the other two protocols only the routing error reporting messages are verified only by the source node.

The Figure 10 below depicts the routing load during the route discovery after the receipt of route error messages in ratio with the number of control bytes per data packet. The routing load is contributed by the packet size in terms of bytes, which is lesser in ARAN while it is more in case of SRP and ARIADNE. In ARAN at every intermediate node the sign of the forwarding node is removed and replace by the current node, whereas in the

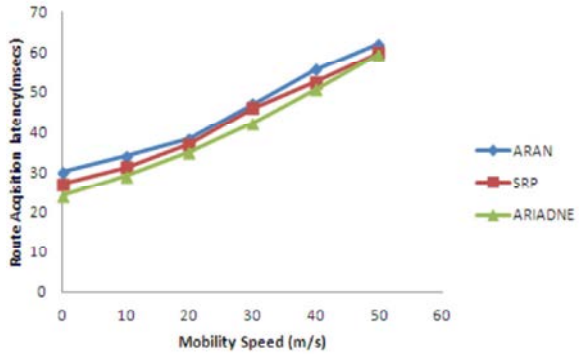

Fig. 7: Route Acquisition Latency

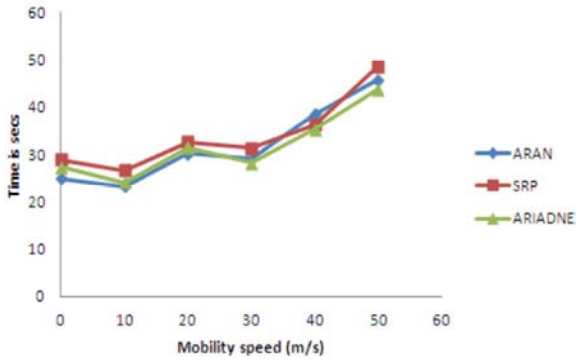

Fig. 8: End to End Delay

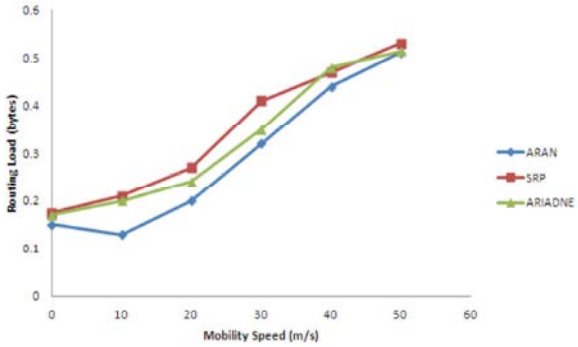

Fig. 9: Routing Load

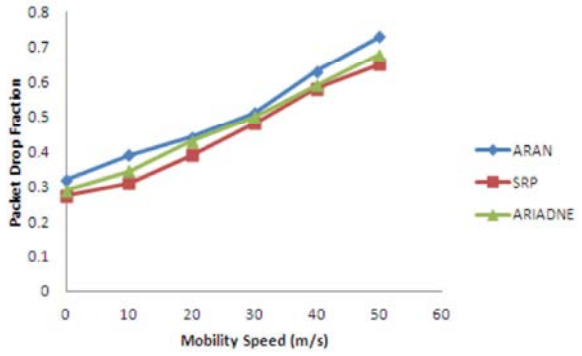

Fig. 10: Packet Drop Fraction

other two the authentication data are appended to the existing contents hence the variation of lesser routing load in ARAN.

Figure 10 represents the fraction of packets dropped computed as the ratio of the number of packets dropped to the number of packets generated at the source during the switch over to alternate route from the current route on receiving RERR messages. No: of packets dropped = No: of packets generated - No: of packets received. Packet drop fraction = No: of packets dropped /No: of packets generated.

Although a negligible variation is shown by the three protocols, higher packet drop ratio is contributed by the time taken by the protocols to resume the communication via the alternate routes.

CONCLUSION

This research study analyzed the role of route cache and route maintenance in Dynamic Source Routing, its security vulnerabilities and three secured versions of DSR viz. ARAN, SRP and ARIADNE. We have given an evaluation of the performance and the responsiveness of the during link breakage and acquisition of new routes to resume the communication by the route maintenance procedure in a normal open environment. In common with all the above three secured protocols, the alternate route to the destination is searched for only after the failure of transmission resulting in some data packet loss, end to end delay and routing load incurred by route discovery. The present work presented the performance of the protocols based on the route maintenance process. Overall ARIADNE and SRP show similar response than ARAN due to computational complexity involved. In conclusion, it is inferred that none of the secured source routing protocols have focused on effective route maintenance which is also one of the key factors that reflect on the performance of the protocols. More of security challenges in the field of reactive routing in mobile ad hoc networks makes it mandatory for research to design an efficient route maintenance and route cache mechanisms to improve the performance of secured DSR protocols. Our further work could be an embedding an effective route cache management scheme in the existing secured source routing protocol. The other open challenges that prevail in the current scenario is to design security measures to thwart impact of the internal attacks on the performance of the routing protocols. Further research can be focused to provide more computationally light cryptography mechanisms to provide better authentication of nodes that can be compatible for multi-vendor mobile devices and reduce computational complexities.

REFERENCES

1. Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine Clay Shields Elizabeth M. Belding-Royer, “Authenticated Routing for Ad hoc Networks”, IEEE ICNP 2002.
2. Anil Rawat, 2007. Prakash Dattatraya Vyavahare and Ashwani Kumar Ramani, “Enhanced DSR for MANET with Improved Secured Route Discovery and QoS”, International Journal of Network Security, 5(2): 158-166.
3. Naseer Ali Husieen+, Osman B Ghazali, Suhaidi Hassan and Mohammed M. Kadhum, “Route Cache Update Mechanisms in DSR Protocol - A Survey”, International Conference on Information and Network Technology, 2011.
4. Johnson, D., D. Maltz and Y. Hu, 2003. The dynamic source routing Protocol for mobile ad hoc networks. IETF MANET Working Group, draft. http://www. ietf.org/internetdrafts/draft-ietfmanet-dsr03.txt,
5. Ramesh, V., P. Subbaiah, N. Sandeep Chaitanya and P. Bhaktavastalam, 2010. “Secured Preemptive DSR(S-PDSR): An integration of SRP and SMT with Preemptive DSR for Secured Route Discovery”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September.
6. Bin Xiao, Qingfeng huge, Edwin H.M. Sha and Chantana Chatrapornchai, “Enhanced Route Maintenance for Dynamic Source Routing in Mobile ad hoc networks”.
7. Kapil Sharma, ‘Cache performance enhancement in DSR protocol based on Cross-layering for Mobile Ad Hoc Network”.
8. Er. Gurjeet Singh, “Performance and Effectiveness of Secure Routing Protocols in Manet”, Global Journal of Computer Science & Technology,Volume 12 Issue 5 Version 1.0 March 2012.
9. Karlsson, Jonny; Dooley, Laurence S. and Pulkkis, Goran, 2012. Routing Security in Mobile Ad-hoc Networks. In: Informing Science and Information Technology Education 2012 Conference (InSITE’12), 22-27 June 2012, Montreal, Canada.

10. Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, 2008. "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, Fourth Quarter 2008
11. Umang Singh, 2011. "Secure Routing Protocols In Mobile Adhoc Networks-A Survey And Taxanomy", International Journal of Reviews in Computing, 30th September 2011. Vol. 7.
12. Jaspal Kumar, M. Kulkarn and Daya Gupta, "Secure Routing Protocols In Ad Hoc Networks: A Review", Special Issue of IJCCT Vol. 2 Issue 2, 3, 4; 2010 for International Conference [ICCT-2010], 3rd-5th December 2010.
13. Khalid Zahedi and Abdul Samad Ismail, "Route Maintenance Approach for Link Breakage Predicttion in Mobile Ad Hoc Networks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 10, 2011
14. Menaka Sivakumar and M.K. Jayanthi, 2014. "Reliability analysis of Link Stability in Secured Routing Protocols", Engineering Journal, Vol. 8, No: 1, 2014.
15. Parul Tomar, Prof. P.K. Suri and Dr. M.K. Soni, "A Comparative Study for Secure Routing in MANET", International Journal of Computer Applications (0975 - 8887) Volume 4 - No.5, July 2010.
16. Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding Royer, "A Secure Routing Protocol for Ad Hoc Networks".
17. Papadimitratos, P. and Z. Haas, 2002. "Secure Routing for Mobile Ad hoc Networks," in Proc. SCS CNDS, Jan. 2002.
18. Yih Chun Hu, Adrian Perrig and David B. Johnson, 2002. "Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks", MobiCom'02, September 23-26, 2002, Atlanta, Georgia, USA.
19. Lavanya, G. and A. Ebenezer Jeyakumar, 2011. "An Enhanced Secured Dynamic Source Routing Protocol for MANETS", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume X, Issue-4, September 2011
20. Chu-Hsing Lin, Wei-Shen Lai, Yen-Lin Huang and Mei-Chun Chou, Secure Routing Protocol with Malicious Node Deection for Ad Hoc Networks, 22nd International conferencne on Advanced Information Networking and Applications, 2008.
21. Menaka, S. and M.K. Jayanthi, 2013. "Effective Stale Routes Management using Preemptive Routing in DSR", World Applied Sciences Journal, 22(11).