ENGINEERING JOURNAL

Article

Reliability Analysis of Link Stability in Secured Routing Protocols for MANETs

Menaka Sivakumar[1,*] **and M. K. Jayanthi**[2]

1 School of Information Technology & Engineering, VIT University, Katpadi, India
2 School of Computer Science and Engineering, VIT University, Katpadi, India
*Email: smenaka@vit.ac.in

Abstract. The prime characteristics of Mobile Ad Hoc Network (MANET) are infrastructure free, absence of centralized authority and dynamic nature of nodes which are more vulnerable to security attacks. Reliability and security are prime issues to protect the information and nodes in a network during communication which has received more research interest in designing a dynamic secured routing scheme. QoS is set of service requirement that needs to be satisfied by the network during the data transmission in the network. From the perception of QoS best effort protocols ensure optimum network operation in an unpredictable mobile environment. The multimedia applications are intolerable towards delay and reliability which are the features of mobile network, hence the potentials of MANET were not utilized in multimedia applications. These issues of delay and reliability of packet transmission in MANET are contributed by the stability of the communication link even during the mobility of the nodes. This necessitates to analyze the performance of various secured routing protocols based on the stability of the communication link in case of mobility of nodes during data transfer. The present study is focused on the comparative analysis on the various secured reactive routing protocols in MANET signifying the connectivity stability during the mobility of the nodes.

Keywords: Communication channel, reactive routing protocols, mobility, security, route cache.

ENGINEERING JOURNAL Volume 18 Issue 1
Received 2 March 2013
Accepted 14 May 2013
Published 14 January 2014
Online at http://www.engj.org/
DOI:10.4186/ej.2014.18.1.65

DOI:10.4186/ej.2014.18.1.65

1. Introduction

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and AOMDV (Ad-hoc On-Demand Multipath Distance Vector). In MANET the nodes are dynamic Mobilic rather than being static and get connected dynamically in an arbitrary manner from time to time which results in a change of topology. Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network During the mobility of the nodes the routes may get disconnected and the route discovery process has to be initiated to sustain the data communication, where the route cache is updated whenever an alternated route is selected or a new route is discovered for the same set of source and destination. Thus, the responsibility of a routing protocol is to find the correct, efficient route to the destination node and also update the new route faster whenever there is a break in the link [1, 2, 3] during data transmission due to the mobility of the nodes.

MANET is used in various applications like emergency search rescue operations, battle field communications between vehicle on movement, where all the communication among nodes should be reliable and secure. Many secure routing protocols have been proposed, which focuses on establishing a secure route, in the route discovery process but no results are being provided for updating of the route cache in the route maintenance phase in order to provide continuous connectivity between the nodes during mobility without compromising the security aspect. The lack of physical protection of nodes, vulnerability of statically configured security mechanism and energy constraints [4] are identified as challenges toward maintaining the connectivity during mobility. This paper briefs about the comparison of the various secured Routing protocols on link reliability between the nodes in mobility during the communication. The rest of the paper is organized as, section 2 discusses the various security attacks occurring in routing protocols, secured routing protocols. Section 3 describes the concept of link stability and section 4 discusses the simulation study and results with section 5 giving the concluding remarks on the results of the study.

2. Security Issues in Routing

2.1. Routing Attacks in MANETs

Routing attacks are caused by injecting fake route request messages, fake routing information and fake link information that is classified into two categories based on the disruption caused by the attack.

i) Route Disruption: Attacks that divert the legitimate data packets from the actual route that to be transmitted.

ii) Resource Consumption: Attacks that consumes the network resources like bandwidth, power, storage such that the resources are not available disrupting the normal data transmission to legitimate users of the network.

The common security attack encountered in resource consumption in mobile network is the Flooding attack. In this the attacker, tries to disturb the route discovery process by sending a large number of RREQ packet to a non-existing nodes.

The major security attacks that disrupt the route are Blackhole attack, Link Spoofing Attack, Worm Hole Attack, Colluding Misrelay attack.

Black Hole Attack: In this, the attacker sends a fake RREP packet establishing a route via the malicious node, thus intercepting the communicating packets passing through the malicious node.

Link Spoofing Attack: This a type of route poisoning attack that advertises a fake link causing the target node to select the attacker as its MPR.

Worm Hole Attack: One of more sophisticated attacks is this worm hole attack. A pair of colluding attackers uses a high speed private network to intrude the network. The pair of malicious nodes record and

replay the packets thus disrupting the authenticity and confidentiality of the message communicated over the network.

Colluding Misrelay Attack: again like worm hole attack uses a pair of attackers to modify or drop packets thus disrupting the routing information.

2.2. Secured Routing Protocols in MANET

Securing the route can be done in two ways, either preventing the attack or detecting and recovering of the attack [5, 6]. The taxonomy of the secured routing protocol in both aspects of prevention and detection is shown in the chart below:

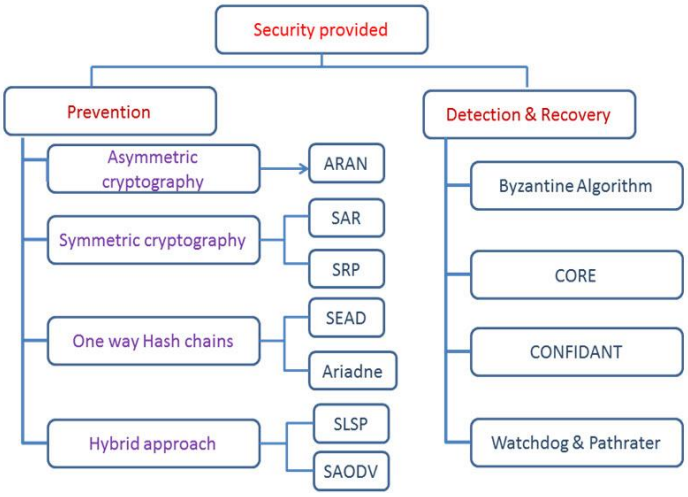

Fig. 1. Taxonomy of secured routing protocols.

Various Researches have proposed many secured routing protocols for MANETs, modifying the routing algorithms embedding with security based measures [7, 8]. Some of the common secured reactive routing protocols existing are ARAN, SRP, SAR, SEAD, Ariadne, SLSP, and SAODV. Each algorithm has various security mechanisms to authenticate the user during the route discovery process. Table 1 gives a brief overview of the security features of the secured routing protocols.

Table 1. Features of Secured Routing Protocols.

Secured Routing Protocol	Cryptography Mechanism	Secret Keys	MAC	Digital Signature	Hash Chain	Verification
ARAN	Asymmetric					Trusted Certificate Server
SAR	Symmetric	Based on trust level specified by the sender				
SRP	Symmetric	SA b/w Src & Dest.	MAC with K_S			MAC
SEAD	One way Hash Chain	Initial Secret Key			Authenticate routing table metric & Sequence number	Hash Chain
ARIADNE	One way Hash chain	Secret MAC Keys	MAC K_{SD}	TESLA Key Authentication		Hash Chain
SLSP	Hybrid (Threshold Cryptography		MAC			MAC Verification
SAODV	Public & Private keys for each pair of users			The sender uses digital signatures to sign the messages	One way hash chain to authenticate hop count	Digital Signature

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. The strength and weakness of the various above mentioned protocols are discussed in Table 2

Table 2. Strength & weakness of 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
SAR	Modification	Dynamic Choice of routes, cost benefit	Not always shortest path is selected
SRP	Detect & Discard bogus replies, fabrication of routing packets	Immune to IP spoofing	Prone to Route cache poisoning, not immune to work hole attack
SEAD	Modification of routing information broadcasting	Efficient in terms of CPU & energy usage	Not immune to worm hole attack
ARIADNE	Modification, fabrication of routing information, flooding	Immune to worm hole attack	Selfish nodes are not taken into account
SLSP	Prevent spoofing at the data link layer	Can operate at recurrently changing topology	Provide assurance only benign control traffic
SAODV	Modification, impersonation	Authenticate in-transit routing packets	Additional storage requirements.

Security extensions for existing routing protocols do not contain important performance optimizations. Inclusion of optimistic approaches provides a better trade-off between security and performance. ARAN (**A**uthenticated **R**outing for **A**d Hoc **N**etworks) and Ariadne are based on DSR of which Ariadne is immune to wormhole attack. Similarly SAR (Security Aware Routing) and SAODV (Secure Ad Hoc On Demand Distance Vector) routing are implemented on AODV while SRP (Secure Routing Protocol) is an algorithm compatible with all the reactive routing protocols [6].

ARIADNE: This reactive secure routing protocol strongly depends on symmetric cryptography. Ariadne uses a shared secret key ($K_{S,D}$) 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. [8, 9]

Point to point authentication using message authentication codes and shared key is a significant feature of ARIADNE. Immunity against wormhole attack and route cache poisoning attacks adds to major strengths of this protocol .

SAODV: The Secure Ad hoc on Demand distance Vector protocol is designed based on AODV routing protocol. This scheme used public key certificates for all the participating nodes in the network. The initiator of the route discovery appends its RSA signature and a last element of hash chain to the routing packets [10]. The intermediate node verifies the signature of the sender before updating the reverse route. The destination node signs the RREP with its private key where the intermediate nodes again verify the sender signature, thus protecting against any illegitimate node getting into the route discovery. The security features provided by SAODV includes integrity, authentication and non-repudiation. [8, 11, 12]

SRP: The Secure Routing Protocol as proposed by P. Papadimitratos et al. [13] is specially designed to be compatible with any of the reactive routing protocols. 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 [8]. 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. A secret symmetric key ($K_{S, D}$) 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 ($K_{S, D}$). SRP scrapes with colluding misrelay attacks, and also replay, fabrication attacks. 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.

All the above discussed secured versions of routing protocols does not possess performance optimizations which could provide a better trade-off between security and performance [14, 15]. On the basis of the comparative study of the secured routing protocols, performance analysis based on link stability in ARIADNE, SAODV and SRP protocols are studied and the results are discussed below.

3. Link Stability

The packet delivery in a MANET relies on the relaying of packets from a source to a series of forwarding nodes until they reach the desired destination. Hence the reliability of these networks depends on the robustness of the link communications between forwarding nodes. In MANETs, a source must establish a route to the destination either proactively or reactively prior to actual data transmissions. In this process, a set of forwarding nodes is selected to form a route between the source and the destination depending on the routing strategy. Due to the mobility of the nodes, this route may remain stable for a finite time period before a link breakage occurs, and link repair or route reestablishment must take place. Figures 2(a) and 2(b) depict a typical scenario of link stability. In Fig. 2(a) data packets are sent from node S to D forwarded via node A. As the destination D moves from the frequency bands of A to frequency band B, the data packets from S take a different route via B.

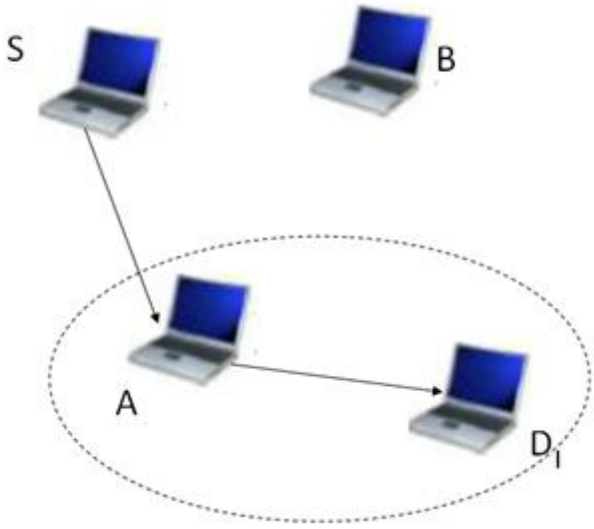

Fig. 2. (a) Initial scenario.

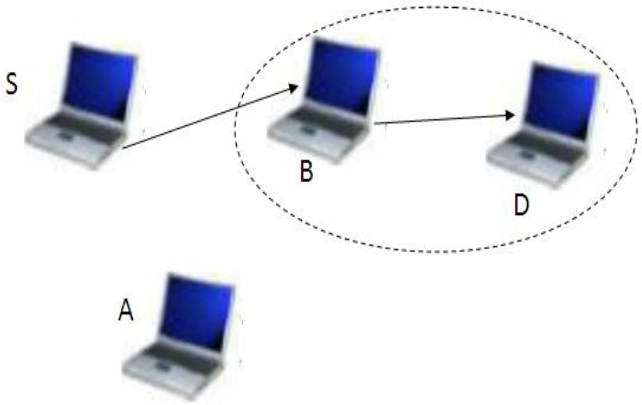

Fig. 2. (b) Changed scenario after mobility of destination.

Inevitably, a brief pause of data transmissions, or more seriously, a disconnection of a communication session between the source and the destination may appear. Hence, prediction of the robustness of a link in

terms of link connectivity duration provides insight to the reliability of the communications and helps improve the routing protocol design.

In this present work, the individual *link stability* is evaluated by modeling the period of time a link between two adjacent forwarding nodes remains connected and the time taken to resume the connectivity in case of disconnection due to mobility of nodes.

Considering all links in an established route between the source and the destination, the *connectivity period*, is further analyzed by measuring the period of time an end-to-end established route remains valid for packet forwarding.

The link stability is analyzed by the time taken from the source to rebuild the route to the destination node after the node has moved to the new location. The time interval between link breakage and link formation which shows the link updating time for the source. The link breakage is identified by the sender and the forwarding nodes on receiving the RERR packet on which the source initiates the route discovery process updating its route cache with the new route. The analysis is simulated for three secured reactive routing protocols SAODV, ARIADNE and SRP using NS2.

4. Simulation Study and Analysis

4.1. Simulation Setup

NS2 simulator is used to study the behavior of the routing protocols and their performance characteristics. The simulation is run for 50 nodes with 45, 30 and 15 connections for all the three protocols and the performance factors like packet delivery fraction, throughput and end to end delay are analyzed along with link stability factor. The network area is taken as 500 square meters. The simulation environment details are given in Table 3.

Packet Delivery Fraction (PDF): The ratio between the number of data packets received and the number of packets sent. Packet Delivery Fraction (PDF) = Total Packets Delivered to destination / Total Packets Generated. Mathematically, it can be expressed as:

$$P = \frac{1}{c}\sum_{f=1}^{e}\frac{R_f}{N_f}$$

where P is the fraction of successfully delivered packets, C is the total number of flow or connections, f is the unique flow id serving as an index, R_f is the count of packets.

Throughput: Throughput is total packets successfully delivered to individual destinations over total time divided by total time. The amount of data transferred from one place to another or processed in a specified amount of time. Data transfer rates for disk drives and networks are measured in terms of throughput. Typically, throughputs are measured in kbps, Mbps and Gbps

throughput=(total no.of bytes received /simulation time)*(8/1000) kbps

End-to-End Delay: It is the ratio of time difference between every CBR packet sent and received to the total time difference over the total number of CBR packets received. It refers to the time taken for a packet to be transmitted across a network from source to destination.

$$\mathbf{D}_{etoe} = \mathbf{N}(\mathbf{D}_{trans}+\mathbf{D}_{prop}+\mathbf{D}_{proc})$$

where $\mathbf{D}_{trans}$ = Transmission delay;
$\mathbf{D}_{prop}$ = Propagation delay;
$\mathbf{D}_{proc}$ = Processing delay;
$\mathbf{N}$ = Number of links [number of routers+1].

Link Stability: The link stability is measured by analyzing the link breakage time and new route acquisition time. The time interval between link breakage and the time of new route acquisition is the time take for routing table to update with the new route to the destination on mobility. The lesser the time taken for updating the route cache with new route interprets how quickly the connectivity break is resumed to maintain the stability of the link. The number of packets dropped is also accounted to estimate the performance of the link reliability during the mobility of the nodes. The number of packets dropped is computed as the difference between the number of packets generated at the source and the number of packets received by the destination node. The following graphs depict the results simulated for the simulation setup discussed in Table 3 for study. The security parameters setup is also given in Table 4.

Table 3. Simulation parameters.

Parameter	Values
Traffic type	CBR (constant bit rate)
Simulation time	100 seconds, 200 seconds
Number of nodes	50
Pause time	0,25,50,75 and 100 seconds
Maximum connections	45
Number of nodes per route	10
Mobility Model	Random Way point model
Topology Size	500m x 500 m

Table 4. Protocol specific parameters.

Protocol	Parameter	Values
ARIADNE	TESLA Time Interval	1 second
	Hash Length	80 bits

4.2. Results and Discussions

SRP, SAODV and ARIADNE secured versions of MANET routing protocols are simulated for the study using NS2. As SRP is compatible with any of the reactive routing protocols it is implemented with TORA for the present study, SAODV is the secured version of AODV while ARIADNE is the secured version of DSR routing protocols respectively. The simulation results of link stability of secured routing protocols are presented in this section and given in Figs 3-7. Figure 3 shows the time of the link being disconnected that the time when the intermediate nodes starts broadcasting the RERR message to the source and the other neighboring nodes.

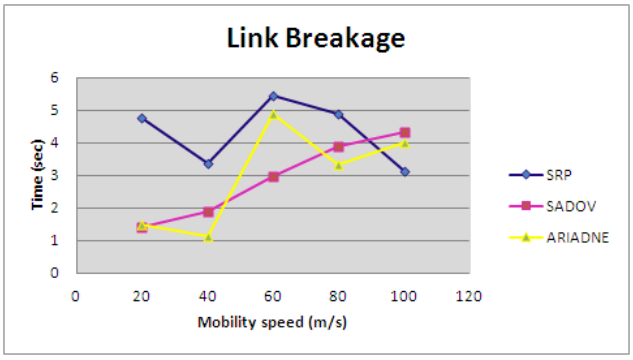

Fig. 3. Link breakage time for the distance moved by the node.

In Fig. 4, the time when the source node resumes the communication via the new route is plotted. Figure 5 shows that the time taken for the route cache to get updated with the new route information increases with the distance moved, on an average compared with the pause time for the mobility and from the graph it is distinct that ARIADNE takes lesser time to update the route cache with new route than SAODV and SRP.

DOI:10.4186/ej.2014.18.1.65

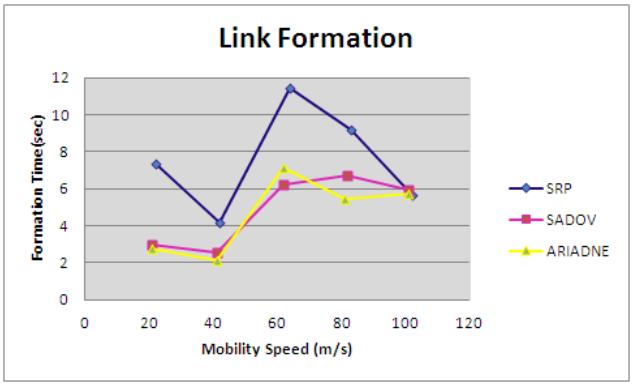

Fig. 4. New route acquisition time.

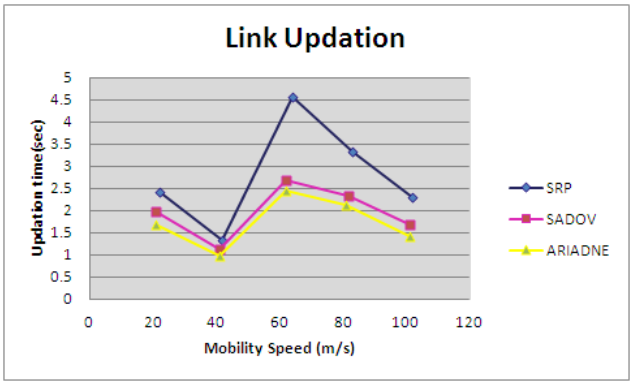

Fig. 5. Time taken to update the new route in the route cache.

Figure 6 shows the updating time almost similar with the distance as a factor. From Figs. 5 and 6 it is evident that ARIADNE performs better than the SAODV & SRP consume less time to update new route to maintain the link stability avoiding packet loss.

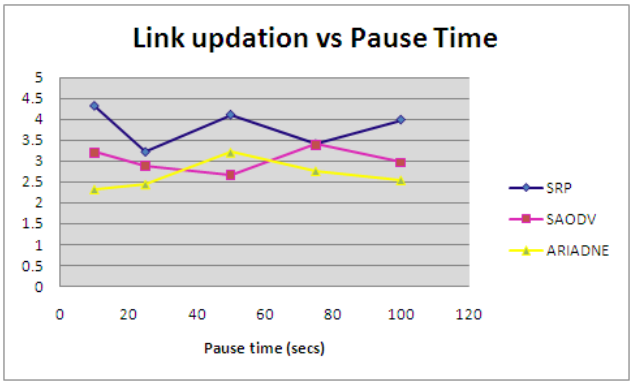

Fig. 6. Time taken for new route updating for various pause times.

The resultant impact on the link stability is shown in Fig. 7, where the number packets dropped is minimized in the case of ARIADNE than the other two protocols. As the pause time is increased more time available for the route updating in case of link breakage and hence the number of packets dropped is also reduced.

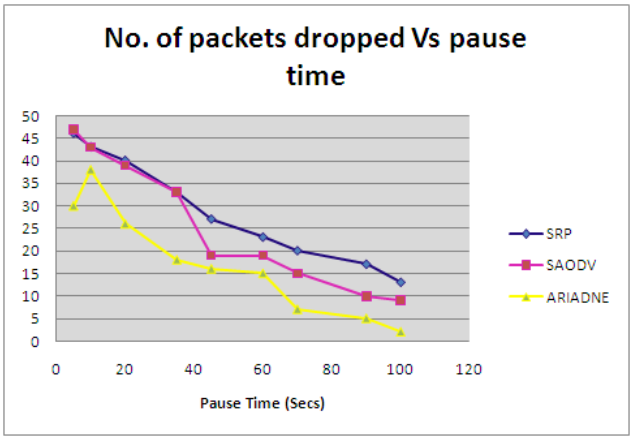

Fig. 7. Packet dropped with varying pause times.

Figures 8 to 10 depict the other performance factors analyzed for the present set of secured reactive routing protocols under study in this paper.

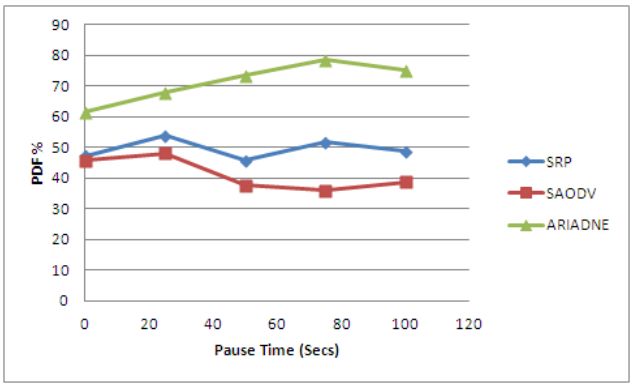

Fig. 8. Packet delivery fraction.

It is evident from Fig. 8 that at pause time 0 sec, ARIADNE has a better PDF value when compared to SAODV and SRP. And also ARIADNE gives better performance with increasing pause time.

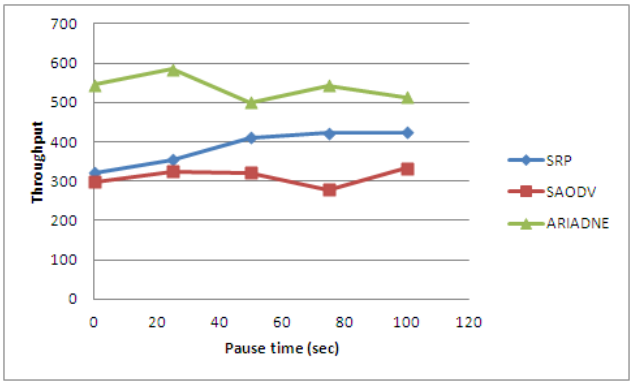

Fig. 9. Comparison on basis of throughput.

DOI:10.4186/ej.2014.18.1.65

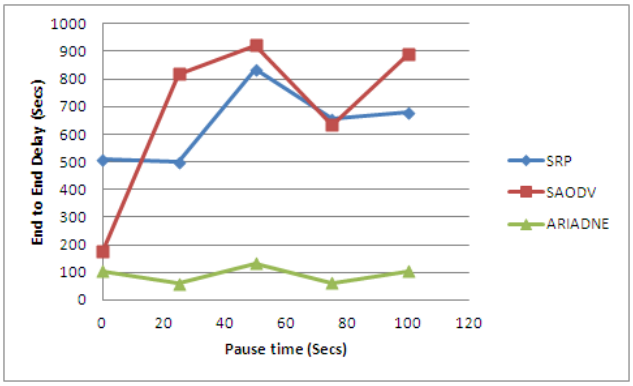

Fig. 10. Comparison on basis of end-to-end delay at maximum connection 15.

The analysis of Figs. 9 and 10 shows that among the three secured protocols ARIADNE, SAODV and SRP, overall ARIADNE gives a better performance in terms of packet delivery fraction, throughput and end to end delay. ARIADNE has a higher percentage of packet delivery and hence increased throughput with minimum end to end delay than SAODV and SRP.

5. Conclusions

This study is done for average networks set up in terms of topology area size, number of the nodes in the move, an average constant mobility speed and fixed number of intermediate nodes per route. Here the assumption is taken as what is the case when the link breakage is due to the mobility of the destination node, while there are situations link may get disconnected either of the source or intermediate nodes also are on move simultaneously during communication and the impact of higher mobility speed the number of nodes per route are not taken into consideration in the present study. From the above results it is distinct that ARIADNE outperforms the other secured routing protocols taken for the present study due to the case of SAODV and SRP the security mechanisms of digital signatures, query identifiers for the establishment of security association etc., are done at every node by itself that consumes time leading to delay in packet delivery while ARIADNE is a single point of certificate authority for authorizing the nodes giving a better performance.

A comprehensive analysis have been carried out on the various security issues in routing the MANET and given a brief overview of the features of the various secured routing protocols designed for MANETs. Further a performance analysis based on the link stability in three of secured routing protocols is presented. The algorithms has its own merits based on the scenario, hence no single protocol could be credited as the best for the network. The selection of the protocol depends on the type of data and network being used for communication, whether more confidential data or whether the nodes are less or more mobile. The small pause time in the data transmission intrudes a small amount delay in packet delivery, which intolerable in multimedia data. The procedures to overcome this packet delay due to link breakage and link updating in case of faster mobility is not yet worked on which is one of the demanding research requirements in MANET routing. There is still a high tradeoff between high security and performance issues like power control, accommodating multiple classes of traffic which are yet to be addressed in designing a good secured routing protocol.

References

[1] L. Qin and T. Kunz, " Increasing packet delivery ratio in DSR by link prediction," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003*, p. 10.

[2] V. Ramesh, P. Subbaiah, and K. Supriya, "Modified DSR (preemptive) to reduce link breakage and routing overhead for MANET using proactive route maintenance (PRM)," *Global Journal of Computer Science and Technology*, vol. 9, no. 5, pp. 124-129, 2010.

[3] Q. Li, C. Liu, and H. Jiang, "The routing protocol AODV based on link failure prediction," in *ICSP IEEE*, 2008.

[4] C. Sreedhar, S. Madhusudhana Verma, and N. Kasiviswanath, "Performance analysis of secure routing protocols in mobile ad-hoc networks," *IJCST*, vol. 3, no. 1, 2012.

[5] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, 2008.
[6] U. Singh, "Secure routing protocols in mobile adhoc networks-a survey and taxanomy," *International Journal of Reviews in Computing*, vol. 7, Sept. 2011.
[7] K. Zahedi and A. S. 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.
[8] M. J. Kumar and K. D. Gupta, "Secure routing protocols in ad hoc networks: A review", in *Special Issue of IJCCT, 2010 for International Conference (ICCT 2010)*, December, pp. 3-5.
[9] G. Lavanya and A. E. Jeyakumar, "An enhanced secured dynamic source routing protocol for MANETS", in *International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307*, vol. X, no. 4, Sept. 2011.
[10] P. H. Phu, M. Yi, and M. K. Kim, "Securing AODV Routing Protocol in Mobile Ad-hoc Networks," in *Active and Programmable Networks*. Berlin Heidelberg: Springer, 2009, pp. 182-187
[11] M. G. Zapata. (2001). Secure ad-hoc on-demand distance vector (SAODV) routing. IETF MANET. [Online]. Internet draft (work in progress), draft -guerrero-manet-saodv-00.txt, [Accessed: 10 October 2006].
[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 21-38, 2005.
[13] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002, pp. 193-204.
[14] K. Sahadevaiah, P. P. Reddy, and G. Narsimha, "A new security protocol for mobile ad hoc networks," *IJCA Special Issue on Communication Security*, no. 1, pp. 9-15, Mar. 2012.
[15] G. Santhi1 and A. Nachiappan, "A survey of QoS routing protocols for mobile ad hoc networks," *International journal of Computer Science & Information Technology (IJCSIT)*, vol. 2, no.4, Aug. 2010.