An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET

S. Ashok Kumar*, E. Suresh Babu*, C. Nagaraju, A. Peda Gopi***
* Department of Computer Science and Engineering, K L University
**Department of Computer Science and Engineering, Yogi Vemana University

Article Info

Article history:

Received Apr 2, 2015
Revised Jun 14, 2015
Accepted Jun 29, 2015

Keyword:

AODV
DSR
MANETs
Routing Protocols
Rushing Attack

ABSTRACT

Over the last decade, researchers had proposed numerous mobile ad hoc routing protocols for which are operate in an on-demand way, as standard on-demand routing protocols such as AODV, DSR and TORA, etc., have been shown to often have faster reaction time and lower overhead than proactive protocols. However, the openness of the routing environment and the absence of centralized system and infrastructure make them exposed to security attacks in large extent. In particular, one such kind of attacks is rushing attack, which is mostly hard to detect due to their inherited properties, that alters the network statistics radically. In this paper, we modeled a rushing attack which is a powerful attack that exploits the weaknesses of the secure routing protocols. Moreover, to know the weakness and strength of these protocols, it is necessary to test their performance in hostile environments. Subsequently, the performance is measured with the various metrics, some ot them are average throughput, packet delivery ratio, average end-to-end delay and etc., to compare and evaluate their performance.

Corresponding Authors:

C. Nagaraju,
Department of Computer Science and Engineering,
Yogi Vemana University,
Vemanapuram, Kadapa, Andhra Pradesh 516216, India
Email: cnrcse@yahoo.com

A. Peda Gopi,
Department of Computer Science and Engineering,
K L University,
Vaddeswaram, Guntur, Andhra Pradesh 522001, India
Email: gopiarepalli2@gmail.com

1. INTRODUCTION:

Wireless communication era has developed greatly over the last few decades, which brought essential changes to the field of telecommunication and networking. Particularly, the wireless and mobile communications have become an integral part of our daily life. However, exchanging the required information with full-fledged wireless connectivity over wireless networks is still an open problem. In this regard, there is a need to establish the instant communication to exchange the information between the wireless devices. Mobile Adhoc network [1] is one such kind of network that provides instant communication between the mobile users which forms a dynamically changed network without any fixed network infrastructure. More importantly, these networks changes dynamically and unpredictably that makes routing as a challenging issue. To address this issue, researchers have proposed numerous routing protocols DSR[2], AODV[3], DSDV, OLSR, TORA, etc. However, the openness of the routing environment and the absence of fixed infrastructure make them exposed to security attacks in large extent. In particular, most of the attacks such as Black hole attack, wormhole attack, rushing attacks, which are particularly hard to detect due to their inherited properties, that alters the network statistics radically.

This paper compares the performance analysis and evaluation of three reactive (TORA, DSR and AODV) protocols in hostile environment. Specifically, the rushing attack will be evaluated against these reactive protocols to validate the performance of the MANET through simulations. Moreover, rushing attack does not consume the lot of resources or cost to subvert the normal behaviour of the network. Particularly, rushing attack is one of the denial-of-service attacks that exploit the vulnerability against standard dynamic routing protocols. In reactive routing protocol, global route discovery procedure is initiated by the originator that generates a route request (RREQ) and forwards the RREQ packets to the neighbour nodes. According to the property, the intermediate nodes will take the first rushed RREQ packet into the consideration and discard the following RREQ packets. The attacker will exploit this property in every dynamic routing protocol to commence the rushing attack.

The related work is here in Section 2. Section 3 discuss about reactive routing protocols. Section 4 briefly explains about rushing attack and Section 5 deals with the performance evaluation of three on-demand routing protocols. Section 6 provides the simulation work. In the end, we conclude in section 7.

2. RELATED WORK

In modern times, numerous resolution are proposed for MANET [4] routing proposals to moderate the trouble of routing interruption. Either symmetric key based protocols (e.g., TESLA [5]) [6] or public key based digital signatures [7] are used to distinguish the genuine members from the strangers. Subsequently network elements reject to agree or forward any unauthorized data packet. Conversely, those cryptographic countermeasures cannot fully respond to the routing commotion challenge. The intrusion detection techniques proposed by Bradley et al [8] and Cheung and Levitt [9] for identifying and detecting routers that forward fake route update message packets. Here, we illustrate one invariant of node performance and present a scattered method to avoid the hosts that have been trapped infringe that invariant.

A multi-path approach studied by Papadimitratos and Haas [10] is to alleviate the route commotion attacks. The message packets are encoded into removal codes, the receiver is able to recuperate the sender’s information only after getting a threshold division of encoding symbols that have been carried along with the multiple paths.

The routing protocol of Perlman’s Flooding NPBR [11] for wired connection networks does not go through this attack, as the procedure does not depend on the genuine path of the overflow for routing; slightly, it have need of that every packet be swamped through the network. Awerbuch et al. [12] proposed an analytical scheme and multi-path evaluation to detect the malicious nodes. If a malevolent node cannot discriminate the information packets without snooping piggybacks from those with, then the originator can recognize the failure range on a route. Though, none of the allied work accepts our restricted approach to protect the best path exposed by the underlying routing protocol. The above proposals are not supported on prescribed models.

3. ON-DEMAND (REACTIVE) ROUTING PROTOCOLS IN MANETs

From the last decade, many routing protocols have been developed for ad-hoc networks by keeping the basic functionalities of routing, which supports the communication over selected paths and transmit the packets over the route. This paper attempts to understand the performance issues of some existing reactive protocols under mobility and varying traffic conditions [13]. Recently a great attention showed towards the on-demand protocols for its potential towards low routing overhead. The on-demand routing protocols are source-initiated that discovers the route as an “as needed” basis instead of conventional proactive protocols. As these routing protocols effectively fulfils the general characteristics of ad-hoc networks such as connectivity against dynamically changing topology, fits the low bandwidth of wireless links [14], quick convergence, etc,. AODV, TORA and DSR are few of the dynamic (reactive) routing protocols which are explained briefly in the following subsections.

3.1 Ad-hoc On-Demand Distance Vector (AODV)

AODV is a dynamic routing protocol that creates and maintains the routes only when they are needed. AODV is composed of two essential functions namely route discovery procedure and route maintenance procedure.

Route discovery: Global Route discovery procedure is initiated when there is no route is available to the target node from the originator. Therefore the source broadcast the route request packets (RREQ) [15] to all the neighbour nodes. On receipt of RREQ, the neighbour nodes create a reverse entry to the originator. The intermediate host receiving RREQ packet will forward to its neighbour and this procedure will go on until the request arrive at the target node. Once the target node receive the RREQ then it response with route reply packet (RREP) over the reverse link towards the originator.

Route maintenance: Once the path is established in between the originator and the target, the route maintenance is introduced to verify the validity of the route because the nodes are arbitrarily move in and out of the network. This protocol makes use of HELLO messages to ensure the routes are active by periodically broadcast the messages between the nodes [16]. If the node in the network does not get a data packet from the intermediate within the stipulated time then the link between intermediate node and itself is considered as broken. This protocol particularly uses the local repair mechanism to rebuild the route towards the destination.

3.2 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is an efficient and simple routing protocol designed for exploit in multi-hop MANETs. This protocol let the network to be utterly self-configuring and self-organizing, without any centralised administration or an active network infrastructure.

The key element of DSR is the use of source routing in which the originator knows the complete sequence order of the nodes in the route to target node and every data packet carries this information in its packet header [17]. The global route discovery and route maintenance are the two important mechanisms of DSR. In Route Discovery, originator broadcasts a RREQ packet that is swamped in a controlled manner all the way through the network and is replied by a RREP (route reply) from either the target node or any other intermediate node that recognize a path to the target node. To decrease the cost of Route Discovery procedure, every node keeps a set of source routes it has overheard or learned which it insistently utilizes to limit the propagation and frequency of RREQs.

The another basic mechanism of DSR is Route Maintenance in which there is no concept of Hello messages which are responsible for periodical updating of routes as like in AODV protocol. It is the responsible for every mobile node of maintaining the routing protocol between the node and next hop in the path from the originator to the target node. In case, if any route from the source is broken, originator is informed with a ROUTE ERROR (RERR). Then the originator tries to make use of any other path to target node already in its route collection or can again initiate route discovery procedure again to discover a fresh route. Route Discovery mechanism and Route Maintenance mechanism both can work completely *on demand* nature and DSR does not require any period packets at any level in the network.

3.3 Temporally Ordered Routing Algorithm (TORA)

The Temporally Ordered Routing Algorithm [18] (TORA) routing protocol is an well-organized, scalable disseminated and highly adaptive routing algorithm proposed for multi-hop and highly vibrant mobile networks. TORA is a sender-initiated dynamic routing protocol that discovers numerous routes from the originator to the target node. The main facet of TORA is that the localization of the control messages to a small set of hosts when the topology of the network is about to change. To accomplish this, the information of routing about their adjacent nodes must be maintained by all the nodes in the network.

The TORA routing protocol has three primary functions such as Route Creation, Route Maintenance and Route Erasure [19]. The first function of TORA is route creation procedure which is responsible for selecting appropriate heights for routers and forming a sequence of links which are directly leading to the target node. The second function of TORA is route maintaining which responds when network topology alters. Since every mobile node must have a particular height, any mobile node with null height is considered as an erased node. TORA protocol has a distinctive quality of maintaining numerous paths to the target node so that the topological changes of the network do not require any response at all. TORA responds only when all the paths to the target node are lost.

4. MODELING A RUSHING ATTACK

Rushing is a zero delay attack shown in Figure 1. It is more dangerous when attacker nearby source or destination. Reactive routing protocols are more susceptible to the rushing attack because whenever source node broadcast the RREQ packets, the attacker or malicious node receives that and forward without any hop-count update and delay in to the network [20]. When legitimate nodes receive original RREQ packets, they are dropped because it already received packet from adversary and treat this as a duplicate packets. Thus, attacker included in active route and disrupts data forwarding. The attacker can gain high speed in access of request by slowing down the response time of other nodes.

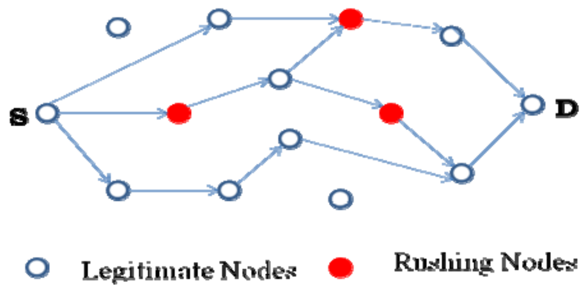


Figure 1. Rushing Attack

The attacker can increase the traffic in network by keeping the network transmission queues [21] full of the nearby nodes. Hence nodes will respond to the request late due to heavy traffic. The authentic nodes will be busy validating request containing false authentications thus slowing down their response ability.

5. PERFORMANCE EVALUATION OF ON-DEMAND ROUTING PROTOCOLS UNDER RUSHING ATTACK

5.1 Rushing Attack Against AODV

In AODV routing protocol the originator node initiate a route discovery for the target node in the network. If the intruder forwards the RREQs and are the first to arrive at each neighbour of the destination, then any path discovered by this global route discovery process will embrace [22] a hop through the intruder. That is, if a neighbour node of the destination node receives the rushed RREQ packet from the intruder, then it forwards that RREQ, and discards any further legitimate REQUESTs from the non-attacking nodes [23]. As a consequence, the originator is unable to find any functional routes. In general words, an intruder node that forwards RREQs more hastily than valid nodes, can boost the probability of that routes that incorporate the intruder will be discovered rather than the other routes.

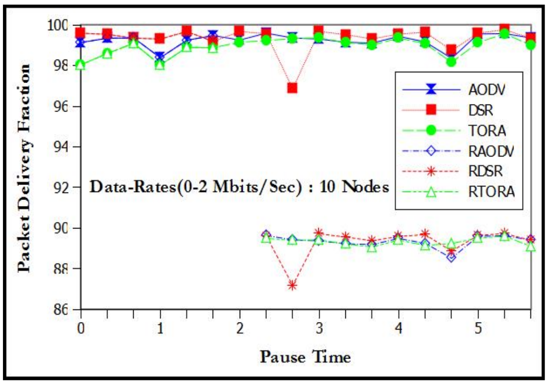


Figure 2. 10-Nodes PDF Vs Pause Time

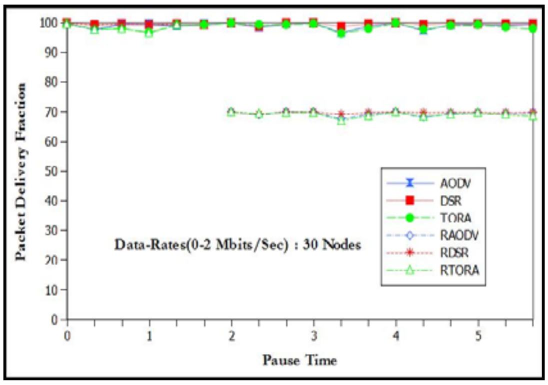
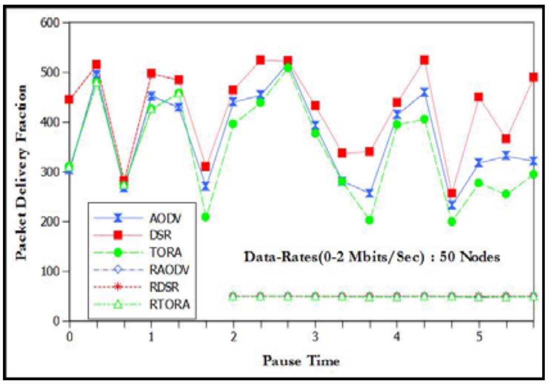


Figure 3. 30-Nodes PDF Vs Pause Time



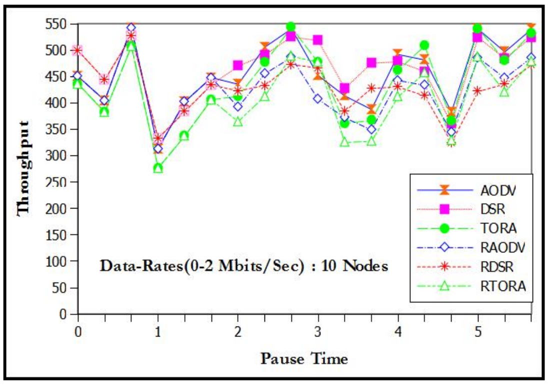


Figure 4. 50-Nodes PDF Vs Pause Time

Figure 5. 10-Nodes Throughput Vs Pause Time

However the above conversation has used the case of mobile hosts in the network that forward just the *first* RREQ from any global route discovery process, the powerful rushing attack can also be used against any routing protocol that inevitably forwards *any* particular RREQ for each global route discovery process.

5.2 Rushing Attack Against DSR

In DSR, the intention of the attacker node is to rush the RREQ to the neighbours of the target node so that it first affects the route discovery mechanism and later it can misbehave the route maintenance mechanism, routing etc. We can discuss the both mechanisms affected by the rushing attack. The Route discovery mechanism contains two segments called route request (RReq) and route reply (RRly). Therefore the rushing attack can take active participation in two phases. In the global route discovery mechanism, a malevolent intermediate node without verifying the route request in its cache, forwards the route request whose aim is to directly rush the route request towards the neighbour of the target node. During the route reply of the destination, the malicious node takes a place as an intermediary node in the route accumulation of the global route discovery process. As a consequence, a path containing rushing node is created between sources to destination in the network. When a neighbour node of the destination gets the rushed RREQ from the intruder, it forwards that RREQ packet. When the valid requests from other nodes appear later at the neighbour hosts, they will be discarded. DSR routing protocol provides a route maintenance mechanism in which it can know that a mobile node is responsible for corroborating that the packet that it forward has been received by the next hop along the legitimate path. If no acknowledgment is received after forwarding the data packet a particular more number of times, this particular node send a route error message (RERR) back to the originator. Since the malicious node is the intermediate node, so it causes the powerful Denial of Service attack by tumbled this route error (RERR) message packet.

5.3 Rushing Attack Against TORA

TORA protocol is proposed for multi-hop and extremely dynamic mobile networks and is a sender-initiated dynamic routing protocol. TORA protocol discovers numerous routes from an originator to a target node. The main facet of TORA protocol is that the control messages are restricted to a small set of hosts when the topology of the network is about to change. TORA is also vulnerable to rushing attack. Due to its openness and lack of central authority, rushing attack is launched in TORA during route creation phase by forwarding QRY message quickly to the target node, when the destination node gets this QRY message it will create route through the intruder node.

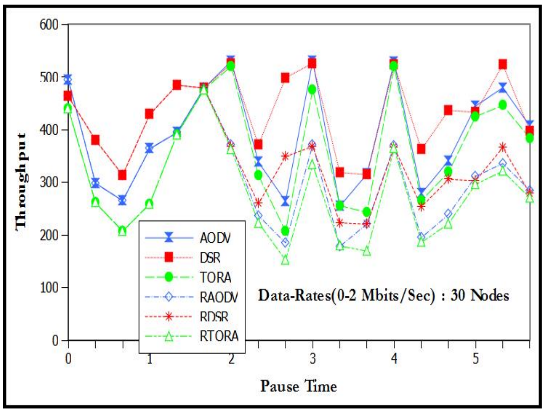


Figure 6. 30-Nodes Throughput Vs Pause Time

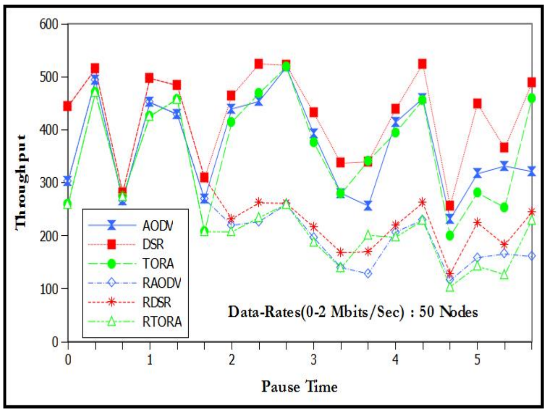


Figure 7. 50-Nodes Throughput Vs Pause Time

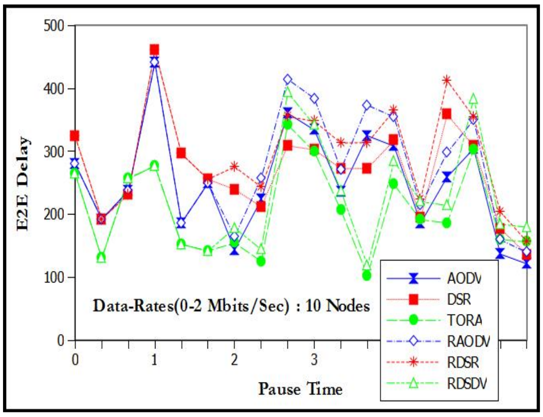


Figure 8. 10-Nodes Delay Vs Pause Time

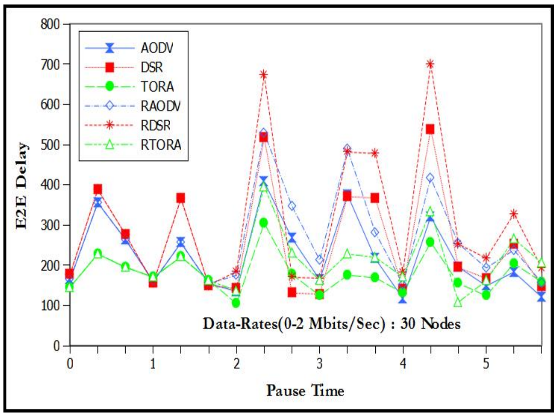


Figure 9. 30-NodesDelay Vs Pause Time

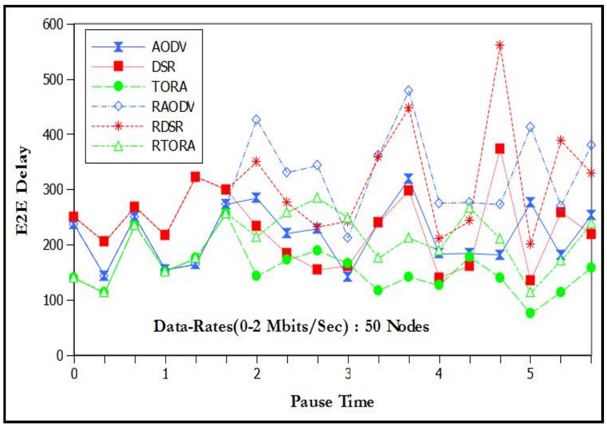


Figure 10. 50-Nodes Delay Vs Pause Time

6. SIMULATION RESULTS AND ANALYSIS

The Network Simulator 2 (Ns-2) tool is used for performing the simulations under the Ubuntu operation system. During the simulation under NS2 tool, every node in the network moves dynamically towards the target node. Once the target node is reached, the mobile host takes a particular period of time (in seconds) for rest and select a new random target node is after that Pause time. During the simulation, this procedure repeats so that continuous topological changes will occur in the network. Different scenarios for different number of mobile hosts and different Pause times are generated.

The results for simulation are given in the above subsection in the graphs. Graphs demonstrate the comparison of the three reactive routing protocols by varying number of hosts on the basis of the performance metrics which are mentioned below.

6.1 Performance Metrics

The performance metrics which are given below are considered for the evaluation of MANET protocols:

1) Packet Delivery Fraction: The ratio of number of data packets delivered to the target node to those produced by the originator.
2) End to End Delay: This represents the time taken for a data packet to move from the originator to the target node.
3) Throughput: This metrics represents the average number of bits arrived per second at destination and measured in bps.

We have observed three reactive routing protocols as already summarized Dynamic Source Routing (DSR) protocol, Temporary Ordered Routing Algorithm (TORA) protocol and Ad hoc On-Demand Distance Vector Routing (AODV) protocol. We have make use of simulations that are given below to evaluate the result .NAM editor which is a network animator to illustrate the animated representation of the three dynamic routing protocols TORA, AODV and DSR, their routing paths and their performances and NS2 network simulator. Moreover, X-graph is used to represent the packet delivery ratio, throughput, and avg. end-to-end delay graphically for the three dynamic routing protocols and therefore comparing them.

Table 1. Simulation Parameters used in NS-2

NS-2 Parameters	
Simulation Time	500 (s)
Number of Nodes	25,50,75,100,125,150
Simulation Area	1000 x 1000m
Routing Protocols	AODV, DSR and TORA
Traffic	CBR(Constant Bit Rate)
Pause Time	10 (ms)
Packet Size	512 bytes
Movement Model	Random Way Point

From the Figure 2, 3 & 4 it is monitored that initially the PDF is very high in the case of AODV when compared with the other two protocols but it reduces significantly if there is increase in the number of simulating nodes. While in the case of DSR simulation the PDF is having high in first situation but it decreases at the starting of the second scenario if the number of simulating hosts increases. PDF in the case of TORA is also increased by the increase in the number of simulating nodes. The PDF of AODV, DSR and TORA routing protocols under rushing attack shows that the packet delivery ratio in these routing protocols adopting similar patterns as increasing the number of nodes due to on-demand nature of these protocols.

In Figure 5, 6 & 7 throughputs illustrate the loss rate and reflect the accuracy and completeness of the dynamic routing protocol. From the above graphs it is very clear that the decrease in the throughput with the increase in nodes mobility. As the packet drop at such a heavy load traffic is much high. TORA protocol shows better performance at the high mobility but in further situations it shows a lower throughput. TORA shows a high throughput when compared to AODV and DSR. Average throughput of the three routing protocols is decrease in the presence of rushing attack but DSR has the less throughput than AODV.

Figure 8, 9 & 10 shows the average end-to-end graphs and from those graphs we have seen that the average packet delay increases with the raise in the number of simulating mobile hosts which are waiting in the interface queue while the dynamic routing protocols make an attempt to discover the path to the target node. DSR and AODV shows the poor delay features as their paths in the network are usually not the shortest. Even if the first global route discovery process discovers the shortest path, that path may not remain the shortest over a time phase due to mobility of the host. TORA protocol too has the worst delay features because of the distance information loss with growth. Also in the TORA protocol path creation may not happen rapidly. This will leads to the possible extensive delays while waiting for the new paths to be resolved. However, for large networks TORA illustrates a superior performance with low mobility rate. The average end to end delay in AODV, DSR and TORA is increase in the existence of rushing attack but delay of DSR in slightly higher than AODV due to cache overhead.

7. CONCLUSION

The past decade witnessed a drastic change in the ubiquitous technology, as researchers proposed several mobile ad hoc network routing protocols which can work in an on-demand fashion. However, the open nature of these routing channels and the absence of fixed infrastructure make them exposed to a large extent of security assaults. Even though a huge amount of time and man power are involved in research, some attacks are still hard to defend in MANETs, One such type of attack is rushing attacks, which are particularly hard to detect due to their inherited properties, that alters the network statistics radically. In this paper, we modeled a powerful rushing attack which is used against three reactive routing protocols. Moreover, we have tested their performance in hostile environments. Subsequently, the performance is measured with the various performance metrics such as throughput, end-to-end delay, and packet delivery ratio etc., As our future work, security solutions for this intrusion is needed for high prospective of sophisticated wireless ad-hoc network.

REFERENCES

[1] S. Basagni, M. Conti, S. Giordano and I. Stojmenovic, "Mobile Ad Hoc Networking", A John Wiley & Sons, Inc., Publication, 2004, ISBN 0- 471-37313-3.

[2] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet draft, February 2002. draft-ietf-manet-dsr-08.txt.

[3] Elizabeth M. Belding-Royer, Charles E. Perkins Evolution and future directions of the ad hoc ondemand distance-vector routing protocol-Elsevier 2003

[4] C.E. Perkins. Ad Hoc Networking. Addison-Wesley Professional, first edition, 2000.

[5] Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes*, 5(2):2–13, 2002.

[6] Y.C. Hu, A. Perrig, and D.B. Johnson. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks. In *ACM MOBICOM*, pages 12–23, 2002.

[7] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E. Royer. A Secure Routing Protocol for Ad Hoc Networks. In *10th International Conference on Network Protocols (IEEE ICNP'02)*, 2002.

[8] Kirk A. Bradley, Steven Cheung, Nick Puketza, Biswanath Mukherjee, and Ronald A. Olsson. Detecting Disruptive Routers: A Distributed Network Monitoring Approach. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 115–124, May 1998.

[9] Steven Cheung and Karl Levitt. Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection. In *The 1997 New Security Paradigms Workshop*, September 1998.

[10] P. Papadimitratos and Z.J. Haas. Secure Data Transmission in Mobile Ad Hoc Networks. In *Second ACM Workshop on Wireless Security (WiSe)*, pages 41–50, 2003.

[11] Radia Perlman. *Interconnections: Bridges and Routers*. Addison-Wesley, 1992.

[12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In *Proceedings of IEEE INFOCOM 2003*, April 2003.

[13] T.P. Kumar, E. Suresh, B.V. Ramana, and B.S. Shashank, "Survey : Routing Protocols in Cognitive Radio Mesh Networks", vol. 6, no. 1, pp. 603–608, 2015.

[14] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. In *Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001)*, Rome, Italy, July 2001.

[15] E.S. Babu, "An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks," vol. 4, no. 9, pp. 691–695, 2013.

[16] E.S. Babu, C. Nagaraju, and M.H.M.K. Prasad, "A Comparative Study of Tree based Vs. Mesh based Multicast Routing Protocols in Mobile Ad hoc Networks", vol. 2, no. 6, pp. 6–11, 2013.

[17] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In *Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*, June 2002.

[18] Vincent Park and Scott Corson. The Temporally Ordered Routing Algorithm for ad-hoc networks.

[19] Adrian Perrig. The BiBa One-Time Signature and Broadcast Authentication Protocol. In *Proceedings of the Eighth ACM Conference on Computer and Communications Security (CCS-8)*, pages 28–37, Philadelphia PA, USA, November 2001.

[20] E.S. Babu and M.H.M.K. Prasad, "An Implementation Analysis and Evaluation Study of DSR with Inactive DoS Attack in Mobile Ad hoc Networks", vol. 2, no. 6, pp. 501–507, 2013.

[21] E.S. Babu, C. Nagaraju, and M.H.M.K. Prasad, "An Implementation and Performance Evaluation of Passive DoS Attack on AODV Routing Protocol in Mobile Ad hoc Networks PROTOCOL OF", vol. 2, no. 4, 2013.

[22] Jogendra Kumar, " Broadcasting Traffic Load Performance Analysis of 802.11 MAC in Mobile Ad hoc Networks (MANET) Using Random Waypoint Model (RWM)", *International Journal of Information & Network Security (IJINS)* ISSN: 2089-3299 Vol.1, No.3, August 2012, pp.223~227.

[23] Yang Shengju*, Shi Shaoting, Zhao Xinhui, “Research on Security of Routing Protocols Against Wormhole Attack in the Ad Hoc Networks”, *TELKOMNIKA Indonesian Journal of Electrical Engineering* ISSN: 2302-4046 Vol.12, No.3, March 2014, pp. 2110 ~ 2117.

BIOGRAPHIES OF AUTHORS

Mr. S. Ashok Kumar received his B.Tech degree in Information Technology from RVR & JC College of Engineering, Guntur, pursuing M.Tech degree in Computer Networks and Security from K.L.University Guntur. He has published 3 research papers in various International Journal. He has attended 10 seminars and workshops. His areas of interests are wireless networks, security issues in MANETs and vehicular networks. He is member of various professional societies like UACEE, IAENG, IACSIT and SDIWC

Mr. E. Suresh Babu received his B.Tech degree in Computer Science from RGM College of Engineering, Nandyal, M.Tech degree in Computer Science from V.T.University Belgaum and pursuing PhD in Computer Science & Engineering from J.N.T.University Kakinada. Currently, he is working as an Associate Professor in the Department of CSE in K L University Vijayawada, He has got 12 years of teaching experience. He has published 8 research papers in various International Journal and 10 research papers in various National and International Conferences. He has attended 32 seminars and workshops. His areas of interests are Wireless Networks, Network Security, and MANETs. He is member of various professional societies like IAENG, CSTA,and CSI .

Dr. C. Naga Raju is currently working as Associate Professor and Head of the Department of Computer Science and Engineering at YSR Engineering College of Yogivemana University, Poddatur, Kadapa District, and Andhra Pradesh, India. He received his B.Tech Degree in Computer Science from J.N.T.University, Anantapur, and M.Tech Degree in Computer Science fromJ.N.T.University Hyderabad and PhD in digital Image processing from J.N.T.University Hyderabad. He has got 18 years of teaching experience. He received research excellence award, teaching excellence award and Rayalaseemavidhyaratna award for his credit. He wrote text book on C & Data structures. He has six PhD scholars. He has published fifty three research papers in various National and International Journals and about thirty research papers in various National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.

Mr. A. Peda Gopi received his B.Tech degree in Information Technology from KLCE College of Engineering, Guntur, pursuing M.Tech degree in Computer Networks and Security from K.L.University Guntur. He has published 5 research papers in various International Journal. He has attended 8 seminars and workshops. His areas of interests are wireless networks, security issues in MANETs and vehicular networks.