I. J. Computer Network and Information Security, **2016, 8, 47-58**
Published Online August 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.08.06

Empirical Performance Evaluation of Reactive Routing Protocols for Wireless Ad hoc Networks in Adversarial Environment

E.Suresh Babu [1]
[1] Research Scholar, JNTUK, Kakinada, KLEF University, AP, India.
E-mail: sureshbabu.erukala@gmail.com

C. Nagaraju [2] **and MHM Krishna Prasad** [3]
[2] Associate Professor, YV University, Kadapa, AP, India
[3] Professor, UEC, JNTUK, Kakinada, AP, India
E-mail: {nagaraju.c, krishnaprasad.mhm}@gmail.com

Abstract—Researchers have already shown the way, how to improve and compare the existing MANET routing protocols that help us to understand the basic feature and functionality of the various routing protocols. However, while these routing protocols have been proposed from different research groups in the literature, which shows the existing routing protocols, are not consistent to common framework to evaluate its performance. Moreover, these protocols are vulnerable to many collaborative attacks, due to its cooperative nature of routing algorithms. Hence, it is difficult for one to choose a proper routing protocol for a given application; therefore, we initially study and review to compare the different existing routing protocols in adversarial environment with varying traffic and mobility simulation scenarios. This paper addresses the comparison of various reactive routing protocols in adversarial environment. To achieve this, we had investigated with widely used NS-2 simulators for fair comparisons of different routing protocols. Furthermore, we also develop a collaborative adversary model for these existing routing protocols that can interfere with communications to subvert the normal operation of the network. Specifically, Our extensive simulation results shows the relative quantitative analysis for comparing the performance of reactive routing protocols such as AODV, DSR under adversarial environments with varying traffic and mobility simulation scenarios. Moreover, the performance of these protocols is measured with the various metrics such as throughput, end-to-end delay, packet delivery ratio, and routing overhead.

Index Terms—AODV, DSR, Heterogeneous Attack, Ad hoc Networks.

I. Introduction

In today's computing world, with the advancement of wireless technology, mobile communication has found its way to improve the living standard of our daily life. The rapidly growing of these technologies permits the users to access the information and service at anytime and anywhere, in spite of their geographic location. These advantages paved the way to resolve the issues such as efficiency, ease to use, and high deployment cost over conventional wired networks. Due to the diversity of applications, there is a necessity, growing interest of future wireless networks, that need to be formed spontaneously, decentralized Infrastructure, and dynamic network architecture had led the development of wireless ad hoc networks.

Wireless Ad-Hoc Networks [1] is one of the self-organized autonomous wireless networks that enable connectivity among any arbitrary group of wireless nodes with no specified geography and time. This also has no need of a centralized access point or existing fixed infrastructure. Such ad hoc networks are suitable where there is a necessity of infrastructure or existing fixed infrastructure is too expensive or inconvenient to employ for applications especially needed by governments, Law enforcement, Emergency scenarios, Military services, Commercial and Civil Applications and vehicular communications etc.

One of the challenge aspects of wireless ad hoc networks in the recent past is the routing issue[6,12,33], due to the dynamic nature and resource constrained, lack of fixed infrastructure, and limited radio range. Therefore, the routing protocols play an important role in wireless ad hoc network communication. Most of the routing protocols in these networks perform two major mechanism, First, Route discovery process, whenever a valid route is not present between the source and the destination node and another mechanism is route maintenance. Whenever, routing algorithms fails to maintain lifelong route between the sending node and receiving node. Moreover, in spite of the routing issue, many wireless ad hoc networks applications require various routing protocols that need to operate correctly even in adversarial environments. The exchanging of sensitive information between the mobile nodes over unprotected wireless links is particularly vulnerable to

different attacks. Thus, deployment of security in these routing protocols of wireless ad hoc networks are still in their infancy, with many security problems unsolved. Security thus becomes a critical issue and poses new challenges that require the design of specialized security solutions. However, this paper presents only the comparison of various reactive routing protocols such AODV[15] and DSR[27] against heterogeneous attack.

The outline for the remainder of the paper is as follows. In Section-II specifies the related work. Section-III discussed routing protocols in mobile ad hoc networks Section-IV specifies the performance comparison of On-Demand Routing Protocol. Section-V built a heterogeneous attack model against ad hoc routing protocols. Section-VI specifies the simulation results and discussion. Finally, we discuss the conclusion with future work in Section-VII.

II. Related Work

Some of the researchers has already focused on comparing protocols that have been presented earlier in the literature. In [2] Park et.al.compared ideal link-state routing protocol with TORA routing protocol. In their comparison, they proved that TORA outperforms ideal link-state. However, this author does not considered mobility. In [3] Broch, Maltz et. al compared four ad hoc routing protocols. They simulated with 50-nodes using different mobility and traffic scenarios. The authors were also used various performance metrics such as number of routing packets Packet delivery fraction and distribution of path lengths They showed that DSR performs better packet delivery, routing load performance, and route length than AODV. However, it performs better only when small numbers of nodes are used. In [4] Charles E. Perkins et.al compared the performance of AODV and DSR routing protocols for mobile ad hoc networks. The authors had demonstrated the performance differentials of these two routing protocols using mobility, varying network load and network size. They believed that DSR outperforms AODV, when less no of nodes while AODV outperforms DSR, when more numbers of nodes and higher mobility. This performance emphasizes the critical need for studying interactions between protocol layers when designing wireless network protocols. However, there is a necessity to validate these protocols in hostile environment. In [5] Tuulia Kullberg presented the scalability and the performance results of the AODV protocol both in large and small networks obtained from different research parties. The author had simulated 50 nodes for the underlying AODV protocol for small networks and found very accurately and efficiently. For larger networks, the author had simulated 10000 nodes with three kinds of improvements such as local repair in addition query localization and expanding ring search for the existing AODV protocol. However, the performance significantly decrease with the number of nodes increases in the network, which indicates poor scalability. In [6] Hongbo Zhou studied various routing protocols in the mobile ad hoc networks. The author had concluded by taking the description and comparison of their various routing schemes, No one protocol cannot fit into all the possible traffic patterns and scenarios of MANET applications due to the strength and weaknesses of the different protocols. The author also addressed current routing protocols lack security mechanisms, which are vulnerable to many attacks. In [7] Rajiv Misra et.al compared the performance of two on-demand routing protocols. In their comparison, they observed DSR out-performs AODV in the constrained situation. While, AODV out-perform DSR in the normal situation. They mainly compared these routing protocols by highlighting local route repairs to overcome from the local congestion situation. In [8] Richard Draves et al., conducted performance evaluation on three link-quality metrics such as per-hop packet pair, per-hop RTT (Round Trip Time) and ETX (Expected Transmission Count). The authors were measured these metrics on DSR routing protocol running in a wireless test-bed. Specifically, they performed experiments using a 23-node static ad hoc network in an office environment, which shows the ETX metric using stationary nodes significantly outperforms the hop-count. However, The Packet Pair metrics and RTT perform poorly because they are load-sensitive and suffer from self-interference. In [9] Mehran Abolhasan et al. Reviewed the comparison of various routing protocols and suggested which routing protocol may perform best in large networks. In their contribution, the authors had categorized into the two types of unicast routing protocols namely, global routing protocols, which makes of traditional link state or distance vector algorithm. Hybrid routing protocols employ both reactive and proactive properties by maintaining intra-zone information proactively and inter-zone information reactively. The authors had concluded that global routing flat protocols could be simple to implement, however it may not scale very well for large networks. While, hybrid routing protocol which is designed network connectivity (proactively) within the routing zones and determining remote route (outside the routing zone) quicker than flooding. In [10]Anurag Kumar et al. discussed on performance of wireless ad hoc networks and they surveyed on the issues such as stochastic capacity, scaling laws, performance of TCP and the Bluetooth performance. They show that in scaling laws, the performance of the network changes with increasing node density. While, they applied stochastic model of wireless ad hoc networks with the assumption of network synchronization along slots. However, this model is impractical to use. In Xukai Zou et al. presented comprehensive review on typical existing routing protocols in wireless ad hoc networks. The author compared by considering various properties with different criteria such as storage complexity, control packet size, time complexity, communication complexity etc., however, there are still many challenges that need to be considered for wireless ad hoc networks. In [11] S. Ramanathan et al. surveyed set of techniques employed in various typical existing routing protocols in mobile wireless networks. The author

mainly discussed the impact of node mobility on routing system design in wireless communication. In [13] Houssein Hallani et al. performed experimental results on typical MANETs with the presence of selfish nodes. The author analyzed the behavior of the nodes with quantifiable measurement such as behavior history of the nodes and reliability on existing AODV routing protocol. Their approach is mainly based on utilization of past behavior of nodes to monitor the effect of selfish and malicious nodes on the

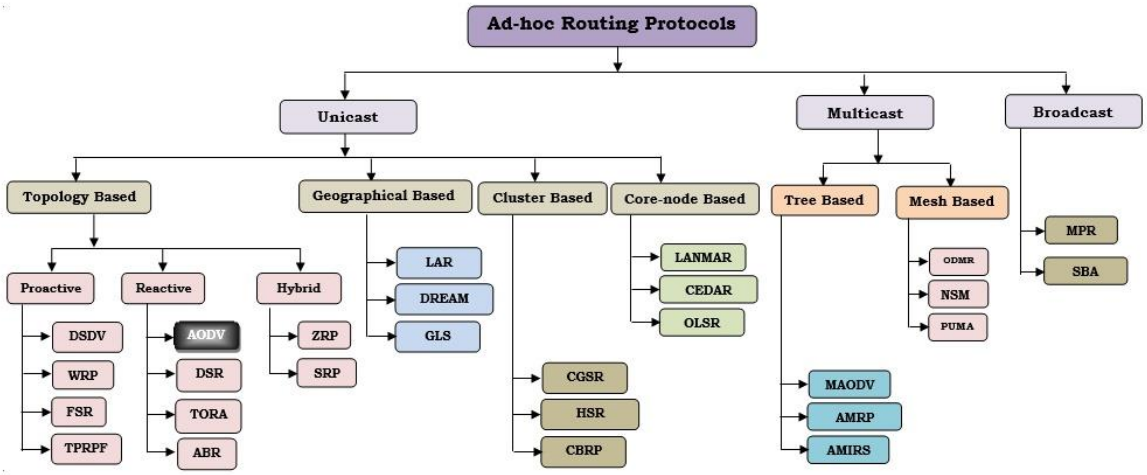

Fig.1. Routing Protocols of Wireless Ad hoc Networks

AODV routing protocols that increases the throughput of around 13% after the discovering the optimal communication paths with a minimal number of selfish nodes or malicious nodes. In Kalyan Kalepu et al. studied functionality of AODV routing protocol under dynamic link conditions. They investigated AODV that affects the performance due to the node mobility. They also showed that the throughput increases as the packet size increases and saturates after a particular value of packet size. In [14] Shideh Saraeian et al. studied DDOS attack that effects the AODV in MANET. In their contribution, black hole attack is used that has high effect on AODV protocol. The author compared with and without black hole attack under AODV with various performance metrics such as PDF which is low under attack and high without attack, End to End Delay not more different with and without attack and Throughput which is low under attack and high without attack. In [3] Josh Broch et.al compared four routing protocols in MANETs AODV, DSR, TORA and DSDV by simulating with 50 mobile nodes. The authors has made two contributions, one is accurate simulation of the MAC and physical-layer behavior of the IEEE 802.11 wireless LAN standard, and the another packet-level simulation comparing four routing protocols of MANETs. They concluded DSDV performs well when node mobility is low and performs poor when node mobility increases. While TORA performance is very poor in terms of routing packet overhead. However, it delivers 90% of packets at 10 and 20 sources. When it comes to the performance of DSR is pretty good at all mobility rates. Finally, AODV also performs almost similar to DSR at all mobility rates. In S.R. Das et al. evaluated the performance of SPF, DSDV, TORA, DSR and AODV routing protocols with various performance metrics such as PDF, End-to-End delay and routing load .The author evaluated for 30 and 60 nodes using MR Simulator. In [16] Azzedine Boukerche et al. had compared the performance of DSR, CBRP and AODV routing protocols using ns-2 simulator. They performance was evaluated with various metrics such as

Average End-to-end Delay, Throughput and Normalized routing overhead with varying pause times and different data sources. Their observation showed CBRP, DSR has higher throughput than AODV. However, CBRP has high routing overhead than DSR. In [26], Tsou et al. introduced a reverse tracing technique to detect and prevent the black hole nodes against DSR routing protocol. In [17], Baadache et al. proposed a novel method based on the principle of Merkle tree to detect the black hole nodes against ad hoc networks. However, their method experiences more computational overhead on routing. In [18], Jain et al. proposed a mechanism for detecting the cooperative malicious nodes based neighborhood monitoring of data blocks between source and destination. In [19], Weerasinghe and Fu et.al introduces a system to prevent the cooperative blackhole attacks in mobile ad hoc networks. However, in their solution, black hole attack can be prevented; the extra control packets will cause more overhead in the network and high latency in the network. In [20] Cheung et al. proposed multiple attacks model and developed a method based on typical isolated alerts about attack steps. In [21] Yang et al. proposed a signature-based mechanism to detect the collaborative attacks. Their technique is based on blind detection techniques, annotated topology information and multicasting. Most of the solutions discussed above are used either to compare the various routing protocol or avoid either black hole attacks or wormhole attack on routing protocols of mobile ad hoc networks. This paper addresses the comparison of various reactive routing protocols under heterogeneous attack.

III. Routing Protocols in Mobile Ad Hoc Networks

The design of efficient routing protocols in mobile ad hoc networks is one of the key challenging research issue. As routing in MANETs particularly difficult to achieve notably because of the inherited unique characteristics such as dynamic topology, low bandwidth, quick convergence and energy, etc., that requires new set of nontrivial function in-contrast to conventional wired and wireless networks. However, in-spite of pleasing characteristics, these networks has certain strength and diverse capabilities such as self-organize, fast deployment and more flexibility than other networks. Form the last decade, researchers had proposed a large class of ad hoc routing protocols that has received more attention towards these networks as shown in Fig.1. However, it is quite difficult to determine which routing protocols may perform best under a number of different network condition's or scenarios. Therefore, In order to know the weakness, strength and distinctiveness of every routing protocol, it is necessary to test the routing protocols performance for mobile ad hoc networks. In an attempt to understand the performance issues better, we have performed comparative performance evaluation of four recently proposed ad hoc routing protocols of two reactive AODV[15], and DSR[27,31] routing protocols of a different nature under varying mobility and traffic conditions with a simulation scenarios.

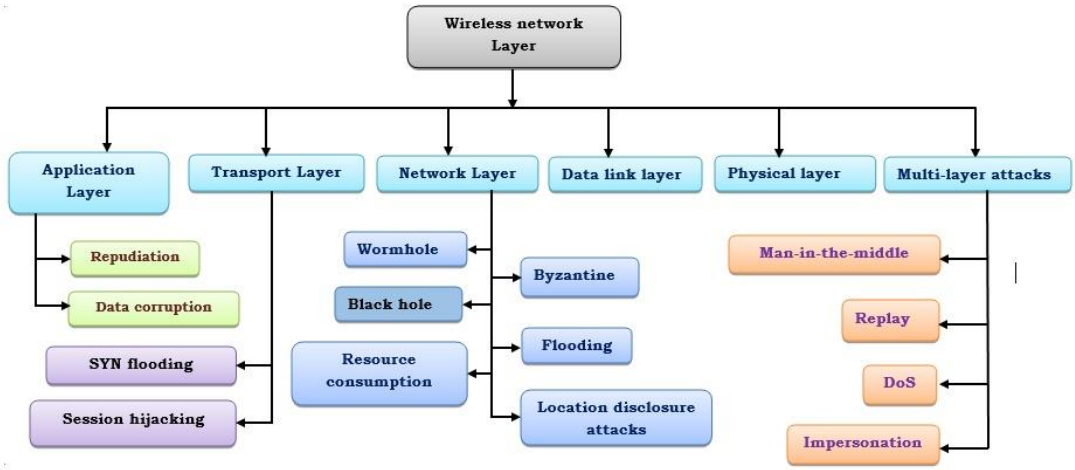

Fig.2. Classification of attacks in Various Layers

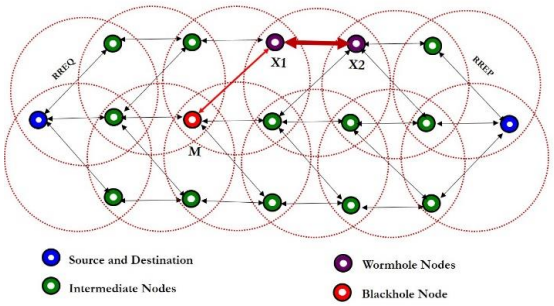

Fig.3. Illustrates the Heterogeneous Attack

A. Ad hoc On-Demand Distance Vector Routing Protocol (AODV).

AODV is the most popular on-demand routing protocol widely used among the research community. This protocol creates the route only when they are needed. Consequently, AODV offers low processing, lo network utilization, quick adaptation to dynamic link changes and low memory overhead. The functionality of AODV is usually performed with route discovery and route maintenance. First, Route discovery process is initiated, whenever a valid route is not present with the source. Therefore, a source node broadcasts RREQ packet to all its neighboring nodes, once the intermediate node receives a RREQ packet from source; it forwards/broadcast the RREQ packet to its next hop. Moreover, the intermediate node creates a reverse link towards the initiator of RREQ, which is used to forward the route replies (RREP) later. This process will be continual until it reaches the destination. Further, if the intermediate or destination node has a valid route towards the destination, then that node is allowed to answer the RREQ with a RREP (Route Reply) by unicast packet through the reverse route backwards of RREQ that had traversed from the intermediate towards originator. Once the route is established between the source and destination, Route maintenance is introduced to check, as AODV fails to maintain lifelong path between the source and destination due to the high mobility by nature. If the link failure results from the mobility, local repair mechanism may be launched to rebuild the route towards the destination. If the local repair is not possible than Route Error (RERR) packet is sent to inform the neighbors nodes about the link failure and informs to the source node about route failure.

B. Dynamic Source Routing (DSR) Protocol.

DSR is also originates from the family of reactive protocol and it was first on-demand routing protocols for MANETs. The key distinguishing feature of DSR is the use of source routing option, which store the complete list

of IP addresses of the nodes along the path towards the destination in its Route Cache instead of routing table contrast to AODV and DSDV routing protocol, Moreover, the source node knows the complete hop-by-hop route information to the destination. This protocol is highly adaptable in resource-constrained MANET's environments, because the routes are discovered only on-demand basis. This basic procedure of this protocol also consists of "route discovery" and "route maintenance" process. First, the "route discovery" process is initiated, when the source node attempts to send the data packets to the destination for which route is not present in the route cache. Therefore, the sender broadcasts the Route Request (RREQ) packets throughout the MANET. Each intermediate node receiving an RREQ rebroadcasts the packet by appending its own IP address in a list in the request packet. Once the destination had received the RREQ packet, then it replies to the RREQ with a route reply (RREP) packet that contains the route information from the source to destination and it is sent back to the original source. The route reply (RREP) packet traverse backwards of request packet that had recorded the source route i.e the request packet has gathered the path (source route) from the source to the destination. Here, both the route request (RREQ) and route reply (RREP) packets contains the route information from the source to destination, which are source routed. Once the path is established between source node and destination node, the delivery of data packets can continue until the topology changes in the network. Suppose the active route link is broken, due to power exhaustion or change in the topology, then intermediate node will notify using a route error (RERR) packet to the source, thus, route link is removed from its cache by the source node and inform other nodes along the route about link failure. Subsequently, the source node reinitiates the route discovery procedure to find a new route if this route is still needed. This whole procedure is achieved through the route maintenance process.

Table 1. Comparison and Characteristic of the Two on-Demand Routing Protocols

Mechanism	AODV	DSR
Neighbor Detection	Yes(Hello Messages)	No
Source Routing	No	Yes
Routing Information Storage	Routing Table (Next hops for desired destination.)	Route Cache (Routes to desired destination.)
Maintenance of Loop Freedom	Sequence Number maintained at each destination node	Source Route
Multi-Path/Route	No(it maintains at most one entry per destination in its routing table)	Yes(it maintains many alternate routes to the destination)
Multicast Capability	Yes (it Support Multicasting MAODV)	No
Route Maintenance	Send RERR, Performs Local Repair	gratuitous route repair – send RERR packet about route link failure, Packet Salvage
Storage Complexity	$O(D_d)$ Where D_d is the number of maximum desired destinations	O(D) Where D: the diameter of the network (the maximum number of nodes in the longest path).
Time Complexity	O(2D)	O(2D)
Control Packet Size	$O(D_d)$	O(D)
Communication Complexity.	0(2N)	0(2N)

IV. Performance Comparison of on-Demand Routing Protocol

In this section, we compared the performance of two prominent on-demand routing protocols for MANETS, because DSR and AODV are the only two competing reactive routing protocols. Even though DSR and AODV routing protocol share similar route discovery and route maintenance modules, but differ in the protocol mechanics such loop freedom maintenance, route storage and neighbor detection, etc. that had led to significant performance differentials. These differentials are need to be analyzed using network size, mobility, routing load and network load. In order to know the weakness and strength of these two on-demand protocols, it is necessary to test their performance. Moreover, this performance comparison gives the state-of-the-art review of two typical on-demand routing protocols for mobile ad hoc networks.

A. Assessment of DSR and AODV Routing Protocol

DSR uses route cache to store its route information of all intermediate nodes. Hence, it can access greater amount of routing information, which is significantly more than AODV. Whereas, AODV uses route table entries to store its route information of all intermediate nodes, which gather only a limited amount of routing information, which is significantly less than DSR. The quality feature of DSR is by virtue of source routing, which significantly reduces the routing overhead than AODV. For Instance, during the route discovery phase, the intermediate node answer with a gratuitous RREP packet about the originator to the destination, if intermediate node is already has the route in its cache towards the destination. Moreover, during the route maintenance phase, the source node piggybacks the gratuitous route repair RERR packet about route link failure in the following new RREQ to inform the other nodes to clean up the caches that may have the failed link in one of the cached source. Whereas, In AODV, only the

source node knows the route information, which limits the intermediate nodes to learn about the route. This usually causes AODV to carry significant routing overhead, because it more often relies on route discovery flooding process.

DSR learns many alternate routes to the destination, which supports multi-paths routing that saves the overhead of route discovery process, whenever the source node receives the RERR packet; it uses the alternative route, which is already stored in its routing cache towards the same destination. On the other hand, AODV maintains at most one entry per destination in its routing table, because the destination node replies with the RREP Packet only once to arriving first request packet and ignores the rest.

AODV uses sequence numbers maintained at each destination node, which always chooses the fresher route. Whereas, DSR do not prefer "fresher" routes because no explicit mechanism is present to handle the expired stale routes in its route cache. AODV perform a timer-based activity at each node, which effectively utilize the individual routing table entries and erases all routes if the link is broken. Whereas DSR do not perform any timer-based activities.

In summary, the following Table-1 gives comparison and characteristic of the two on-demand protocols

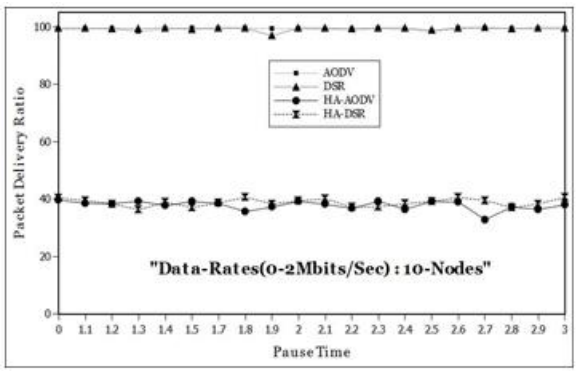

Fig.4. Packet Delivery Ratio vs Pause Time between AODV and DSR for 10-Nodes under Heterogeneous Attack

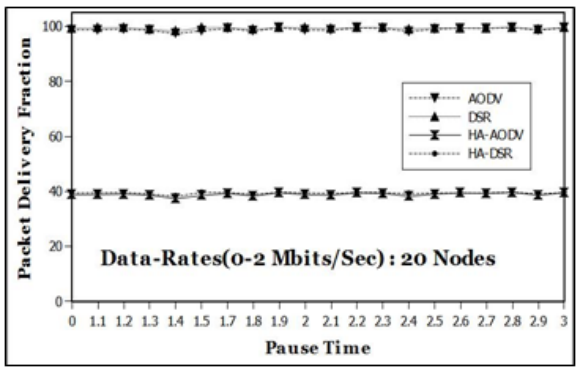

Fig.5. Packet Delivery Ratio vs Pause Time between AODV and DSR for 20-Nodes under Heterogeneous Attack

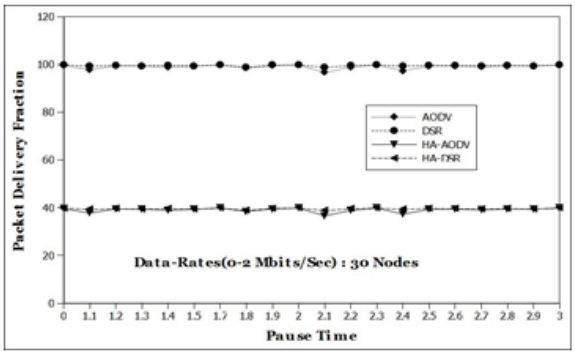

Fig.6. Packet Delivery Ratio vs Pause Time between AODV and DSR for 30-Nodes under Heterogeneous Attack

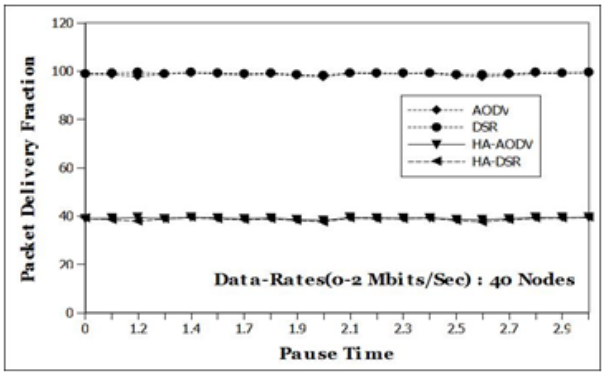

Fig.7. Packet Delivery Ratio vs Pause Time between AODV and DSR for 40-Nodes under Heterogeneous Attack

V. Modelling Heterogeneous Attack Against Adhoc Routing Protocols

Over the last few years, various research works have been conducted by the researchers to address most prominent, well-known attacks such as Black hole, Worm Hole, Sinkhole, Rushing, Man-in-the-Middle, Gray Hole attacks, etc., as shown in Fig.2 against numerous ad hoc routing protocols in an isolated fashion. While, these attacks tries to either disturb the routing operation and deny the services to legitimate nodes or attempt to completely terminate all activity, due to the inherent characteristics that exploit vulnerabilities of ad hoc networks. However, Most of such efforts have been put on mechanisms to deal with individual attacks and these mechanisms are analyzed and evaluated by separate simulation experiments. According, the performance metrics are chosen for a specific purpose. This section mainly addresses the Heterogeneous Attack, which may cause more devastating impacts on ad hoc networks than single and uncoordinated attacks. In general, the heterogeneous attack model was developed to investigate the weaknesses of the routing protocols of mobile ad hoc network that exploits the vulnerabilities of ad hoc environments, which will harm the system and results in a vulnerability assessment. This Heterogeneous Attack

makes use of the combined efforts of more than one attacker against the target victim. Moreover, this attack may launch multiple intruders to synchronize their activities and accomplish the usurpation, deception, disruption destruction, modification of data, and disclosure against targeted routing protocols to deny the services to legitimate nodes and completely terminate all activity to the network entities. Before, we discuss the working process of heterogeneous attack, let us outline and give a brief introduction of each attack against reactive and proactive routing protocols. (1) Black hole attack [26, 29, 30] can be defined as a Denial of Service attack, in which each black hole node impersonates the source node and destination node by sending a spoofed route request to the destination node and spoofed route reply to the source node that was taking place in route discovery phase to claim that he has the optimal route information. Finally, the black hole node consumes the packet, and simply drops the packets to introduce high end-to-end delay into the network and to degrade the performance of the network. (2) The wormhole attack [25] is one of the collaborative attack, in which an attacker can intercept the packets at one location in the network and quickly guide the Packets to another location with the help of the tunnel and retransmits them there into the network. (3) In DoS attack, the intruder may prevent some of the legitimate nodes from receiving data and control messages by interfering with their radio. (4) In rushing attack [22,25], the intruder does not consume the lot of resources or cost to subvert the normal operation of the network. Particularly, this attack will exploit the vulnerability against on-demand routing protocols. In an on-demand routing protocol, the route discovery process is initiated by the originator in the form of route request (RREQ) and forward the RREQ packets to the neighbor nodes. The malicious nodes forward this RREQ packet more quicker (first rushed RREQ packet) than the legitimate nodes asking for a route to the destination node, and the intermediate or destination node will discard the following RREQ packets. Currently all proposed on-demand routing protocols will accept only first request and accepts only almost one request from any Route Discovery. Accordingly, the attacker will exploit this property in all the on-demand route discovery protocols to initiate the rushing attack. Moreover, two rushing attackers may employ a powerful wormhole attack.

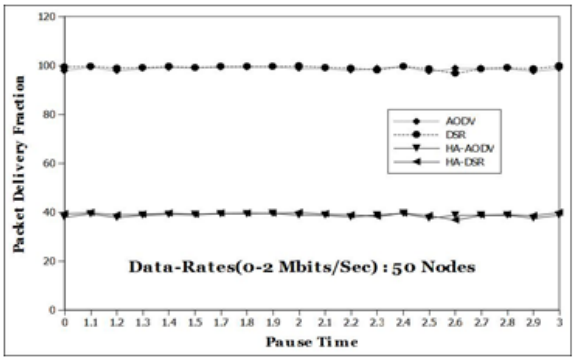

Fig.8. Packet Delivery Ratio vs Pause Time between AODV and DSR for 50-Nodes under Heterogeneous Attack

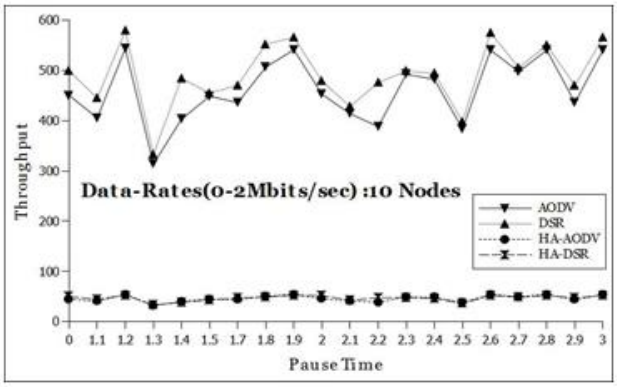

Fig.9. Throughput vs Pause Time between AODV and DSR for 10-Nodes under Heterogeneous Attack

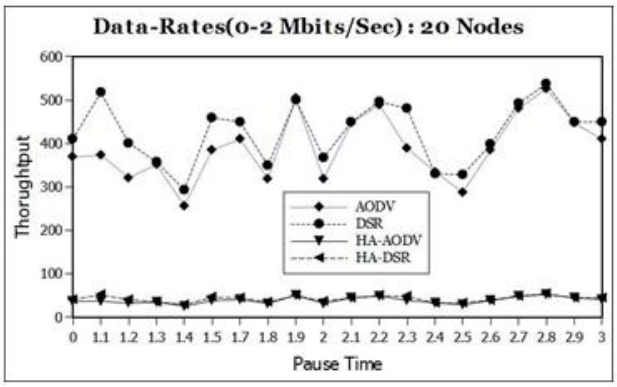

Fig.10. Throughput vs Pause Time between AODV and DSR for 20-Nodes under Heterogeneous Attack

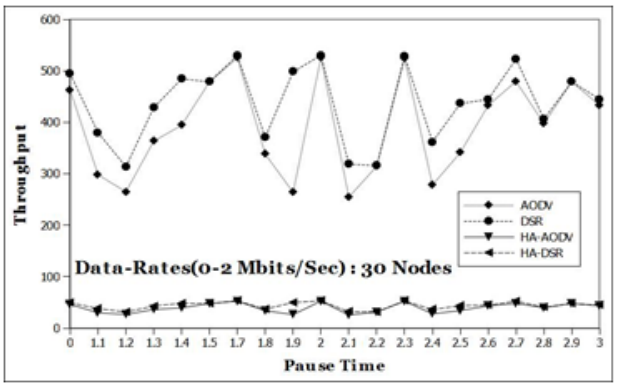

Fig.11. Throughput vs Pause Time between AODV and DSR for 30-Nodes under Heterogeneous Attack

For instance, the first intruder simply forwards the all RREQ packets to a second intruder in the network, which forms a tunnel. If this tunnel affords significantly faster transit than legitimate forwarders, then it will generally discover routes through this tunnel only, which may launch wormhole intrusion. (5) Man in the Middle Attack [23], in this, the attacker can put himself in the middle of a communication by impersonating both the source node and destination node by creating bogus RREQ and bogus RREP messages with its victim's address as originator as well as targeter. The attacker also generates false RERR messages in the network, to proclaim that the target node is not reachable any more. For Instance, the attacker first needs to create its own routes towards the source and

destination nodes using route request packet. Once these routes are established, it can periodically send bogus route reply packet to source and destination. First, the attacker sends the bogus route reply packet with high enough sequence numbers towards source node have the destination field set to target address. So that source node believes that, it is newer information and also trusts they were generated by destination node and thus that a route towards the destination is available through the attacker (MITM) nose just by updating the routing tables. Similarly, the attacker sends bogus route reply packet with originator address to the intermediate node. Thus, the intermediate node records a new route to source node with attacker in the middle as next hop, and destination node records a new route to source node with attacker in the middle as next hop. Subsequently the traffic will flow through the new route, in which the attacker can modify eavesdrop or drop the traffic.

On the other hand, In heterogeneous attack, the attackers are tends to become more and more advanced with the combinations of powerful attacks such as black hole attack, wormhole attack, rushing attack and MITM attacks. Some of the combinations of attacks are: (a) black hole nodes are coordinated with wormhole node. (b) Two cooperate black hole nodes are coordinated with wormhole attack[32]. (c) Rushing attack is coordinated with wormhole node. (d) Attackers are coordinated with black hole; rushing attack and wormhole node (e) rushing attack are coordinated with MITM attack.

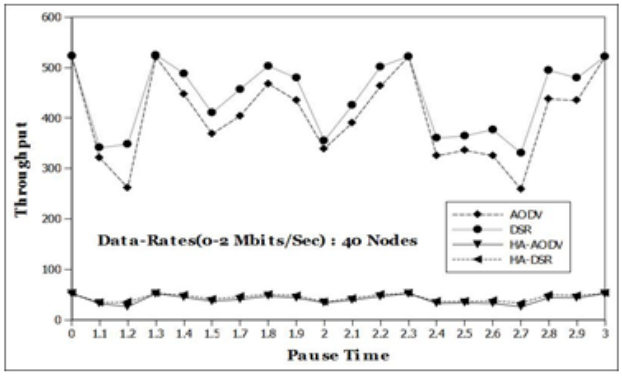

Fig.12. Throughput vs Pause Time between AODV and DSR for 40-Nodes under Heterogeneous Attack

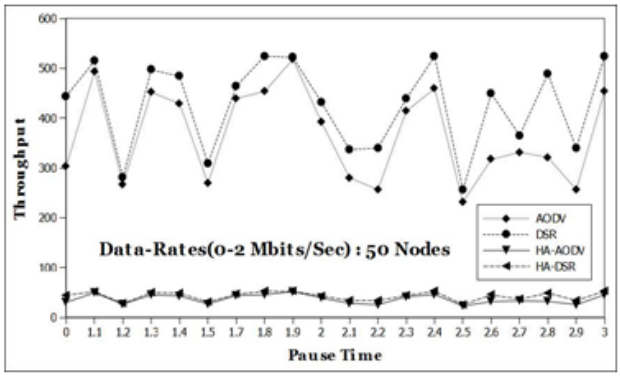

Fig.13. Throughput vs Pause Time between AODV and DSR for 50-Nodes under Heterogeneous Attack

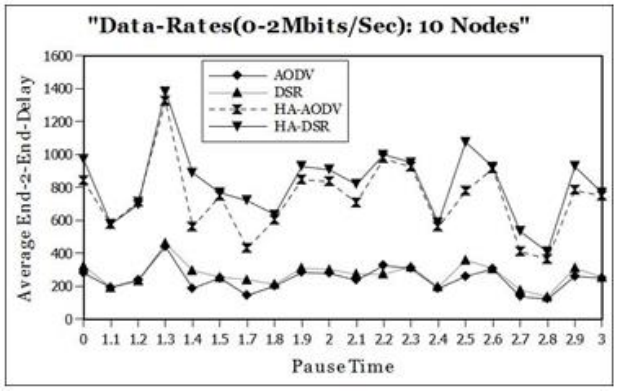

Fig.14. Average End-To-End-Delay vs Pause Time between AODV and DSR for 10-Nodes under Heterogeneous Attack

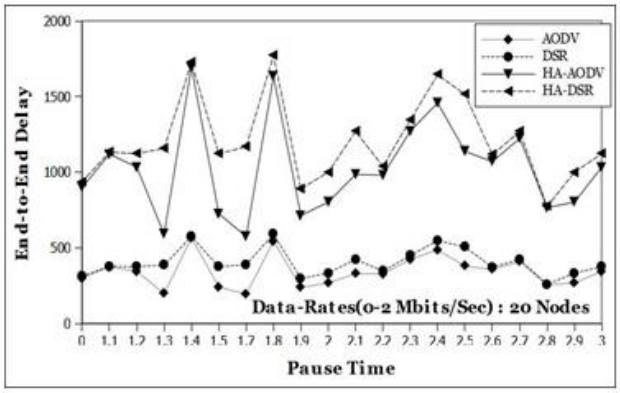

Fig.15. Average End-To-End-Delay vs Pause Time between AODV and DSR for 20-Nodes under Heterogeneous Attack

Let us illustrate with an example, how the different attack are take place simultaneously to form heterogeneous attack. As shown from the following Fig.3. We assume that the source node‘s’ sends the RREQ message to the destination node ‘d’ via some intermediate nodes. We assume that the one of the intermediate node ‘M’ perpetrates a black hole attack. Similarly, the intermediate nodes ‘X1’ and ‘X2’ collude each other to carry out as wormhole attack. Here both M and ‘X1’ is compromised during the route discovery phase and collaborate each other. For instance, the malicious node ‘M’ could not tamper the RREQ message that was received from source, and simply replies with a RREP packet stating that has the shortest path to destination node ‘D’. Then the malicious node ‘M’ will establish a route through the intermediate node ‘X1’ which in turn forward the packets to another node ‘‘X2’ with the help of the tunnel and retransmits them there into the network. After the route discovery setup, the malicious node ‘M’ could not tamper or drop the message that was received from source, but, may forward the message to ‘X1’ node, then the malicious node ‘X1’ and ‘X2’ receives every packet from the black hole node ‘M’ and they can tamper the contents or simply drop them selectively. This specific example illustrates that such a heterogeneous attack which is more devastating on ad hoc networks. Finally, we compared its performance with different two on-demand routing protocols such as DSR, AODV under heterogeneous attack. Moreover, the performance of

these protocols is measured with the various metrics such as throughput, end-to-end delay, packet delivery ratio, and routing overhead.

VI. Simulation Results and Performance Analysis

To study the feasibility of our theoretical work, we have implemented and evaluated the two routing protocol against heterogeneous attack method in network simulator [NS2][28] which is a software program running in Uduntu-13.04 and conducted a series of experiments to evaluate its effectiveness. The experiment results show impacts that are more devastating on these two routing protocols against heterogeneous attack.

The experimental values were obtained by evaluating the current version of the AODV, DSR routing protocol, by including the behavior of heterogeneous nodes into the simulations. Our simulations are mainly used to compare these two routing protocols with and without the presence of heterogeneous attack. To evaluate these four routing protocols, we considered various performance metrics.

a. *Packet Delivery Ratio (PDR):* It is the ratio between the number of application layer data packets that are received correctly by all the destination node, and the number of application layer data packets originated by the source node.
b. *Average End-to-End-Delay:* The Average delay is usually measured in all the correctly received packets. The average time taken to deliver a data packet from the source node and the time taken to be received a data packet at the destination.
c. *Routing Overhead:* The total number of application layer data packets that have been received by the destination node at a given simulation time t.
d. *Throughput:* The total amount number of data packets, which reaches the receiver that have been delivered by the application layer (source) within given simulation time.

Table 2. Parameters used in NS-2 used for Performing Two On-Demand Routing Protocols

NS-2 Parameters	
Propagation model	Two Ray Ground
No of Nodes	10, 20, 30,40,50
Transmission Range	250m
Simulation Time	500 Seconds
Routing Protocol	AODV,DSR
Simulation Area	750m X 750m
Node Mobility	Model Random Waypoint
Traffic Type	FTP/TCP
Data Payload Size	512 Bytes/Packet
Node Pause Time	0-20s
Maximum node speed	0-20m/s

As shown in Table-2. we used various parameters for simulating routing protocols in NS-2. It is worth noticing that, NS2 simulations offers Two Ray Ground, which is a Radio Propagation Model for forecasting the wireless signal strength and Mobility Model, which is used to generate movements of the stations (nodes) within a flat terrain. At this point, we used random waypoint model within a rectangular field with 750m X 750m configurations are used for 10, 20, 30, 40, 50 nodes respectively. Subsequently, A mobility pattern in random waypoint model specifies the certain rules to the mobile node to follow during the motion i.e. the nodes can move either randomly (free movement) or according to the constrained movement, However, these nodes allows the pauses during the mobility. There are numerous mobility models shown in the literature [24] to customize them to the needs of the researcher's. To run the simulations, the simulated time taken is 500s for 10, 20, 30, 40 and 50 nodes with identical traffic and mobility scenarios are used across the routing protocols. The traffic type used here is File Transfer Protocol (FTP), which is a traffic source with the assumption of source and destination pairs are randomly spread across the network. The number of sources, destination-source pairs and the data rate in each pair is varied to change the obtainable load in the network. Another parameter used here is size of data payload of 512-byte data packets only. Moreover, each data packet begins its journey from a source, which is present at one random location and reaches to the destination, which is located at different random location with a randomly chosen speed (uniformly distributed between 0–20 m/s). Finally, we vary the different node pause time that affects the relative speeds of the mobiles. Eventually, these simulations has carried several important characteristics affecting the performance on these routing protocols against heterogeneous attack, however, most of the work has already been analyzed only on these routing protocols and still there is a worth to consider few points, which will be discussed next.

In our first scenario, the experimental values were obtained by using different numbers of sources with a moderate data rate and varying pause times. Moreover, we collect the simulated data by running the simulation up to 500 second with an input of 10, 20, 30, 40 and 50 nodes with different 3, 5, 7, 9, and 12 traffic sources at a data rate of 3 packets per seconds. The Fig. 4, 5, 6, 7 and 8 shows the packet delivery fraction for AODV and DSR. For the 10, 20 and 30 nodes, the PDFs for AODV and DSR are almost similar with 3, 5, and 7 sources, DSR outperforms AODV at higher pause times and for 40 and 50 nodes with 9 and 12 sources, AODV performs better than DSR at lower pause times without the behavior of heterogeneous attack. While from the same figures, it can be seen that the number of packets dropped for 10, 20, 30, 40 and 50 nodes between source and destination is above 65% worst for all pause times, with the presence of heterogeneous attack (in this case black hole, wormhole attack). Here, the number of misbehaving nodes is collaborative in nature, which continues to disturb the routing information and just dropping of packets instead of reaching to the destination, which is more devastating Denial of service.

The Fig.9, 10,11,12 and 13 depicts the throughput of DSR and AODV routing protocol without the presence of heterogeneous attack. We collect the simulated data of 10, 20, 30, 40 and 50 nodes with different 3, 5, 7, 9, and 12 traffic sources at a data rate of 3 packets per seconds. DSR outperforms than AODV for all pause times. However, as the number of nodes in the network grows from 10 to 50 nodes, both the DSR and AODV significantly reduce to deliver the packets to the destinations. Hence, the overall throughput decreases dramatically. The figure also shows that both the DSR and AODV drastically decreases the throughput in the presence of 10% black hole nodes (i.e. one black hole node) and 10% wormhole nodes (i.e. one wormhole node), which are collaborative to each other to form heterogeneous attack with varying pause time, that affects the overall throughput from 65% to 87.5% of the data packets. Moreover, AODV and DSR fail to delivers the data packets and routing packets to the destination. However, DSR provides the relatively better throughput than AODV. i.e the impact on AODV observed was a decrease of approximately seven percent (7%) approximately under the attack. Hence, In AODV, the attacker is more effective in disturbing the routing information than DSR.

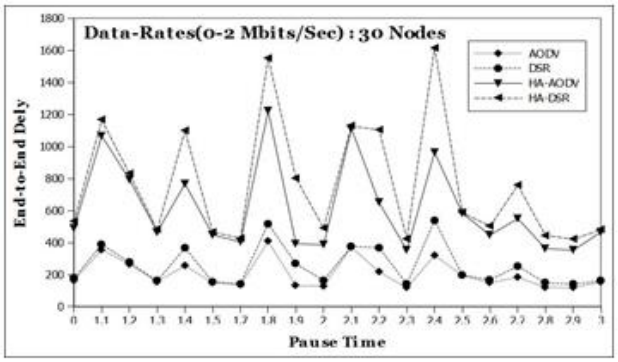

Fig.16. Average End-To-End-Delay vs Pause Time between AODV and DSR for 40-Nodes under Heterogeneous Attack

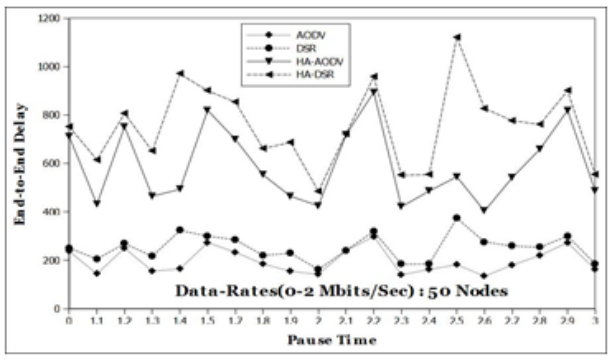

Fig.17. Average End-To-End-Delay vs Pause Time between AODV and DSR for 50-Nodes under Heterogeneous Attack

The Fig.14,15,16 and 17 depicts the Average End-to-End Delay of DSR and AODV routing protocol without the presence of heterogeneous attack. For the 10, 20, 40 and 50 nodes with varying pause time, AODV have lower delay (around 20%) than DSR with varying number of traffic sources. However, it is also notice that for lower mobility DSR is better than AODV, because it does not support any kind of load balancing. To be more specific, let us have a detailed interpretations of the average end-to-end delay results for 10, 20 nodes, the delay is around 0.3 seconds for DSR and 0.2 seconds for AODV with lower pause time. Similarly, for 40 and 50 nodes the average delay is around 0.8 seconds for DSR and 0.5 seconds for AODV with lower pause time. On the other hand, the same figures also shows that both the DSR and AODV drastically increases the average end-to-end delay in the presence of 10% black hole nodes (i.e. one black hole node) and 10% wormhole nodes (i.e. one wormhole node), which are collaborative to each other to form heterogeneous attack

VII. Conclusion and Future Work

In this paper, we addressed the comprehensive performance evaluation and comparison of various ad-hoc routing protocols in hostile environment for mobile ad hoc networks. Moreover, we evaluated the performance of these protocols with various metrics such as throughput, end-to-end delay, and packet delivery ratio across various mobility and traffic scenarios. According to the simulation results, two on-demand protocols (DSR and AODV) showed significantly more efficient in savings the communication overhead. However, these on-demand protocols performs below ideal performance in data packet delivery and end-to-end delay because these protocols are more prone to data packet drops and they will create and maintain routes only on an “as needed” basis. As a result, these on-demand routing protocols is preferred in many applications. Moreover, I also develop a collaborative adversary model against these existing routing protocols that can interfere with communications to subvert the normal operation of the network. Once again, we performed extensive simulation to evaluate the performance of reactive against heterogeneous attack with varying traffic and mobility simulation scenarios. The degree of impact of such attack type differs significantly than single or isolated attack. As work future work, these protocols lack in security mechanisms, which are vulnerable to many collaborative attacks, due to its cooperative nature of routing algorithms. Thus, deployment of security in these routing protocols of wireless ad hoc networks is a critical and challenging issue that requires specialized security solutions.

References

[1] Frodigh, P. Johansson, and P. Larsson, “Wireless ad hoc networking — The art of networking without a network,” vol. 4, no. 4, pp. 248–263, 2000

[2] Park and S. Corson. “A performance comparison of TORA and ideal link state routing”, In Proceedings of IEEE Symposium of Computers and Communication, June 1998.

[3] Broch, D. a. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, “A performance comparison of multi-hop wireless ad hoc network routing protocols,” Proc. 4t

Annu. ACM/IEEE Int. Conf. Mob. Comput. Netw. - MobiCom '98, pp. 85–97, 1998.
[4] Charles E. Perkins, Elizabeth M. Royer and Samir R. Das and Mahesh K. Marina " Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks" published in IEEE Personal Communications-February, pp. 16–28, 2001.
[5] Kullberg, "Performance of the Ad-hoc On-Demand Distance Vector Routing Protocol". 2004.
[6] Zhou, "A Survey on Routing Protocols in MANETs", 1-22,Vol no.1, 2003.
[7] Misra and C. R. Mandal, "Performance comparison of AODV/DSR on-demand routing protocols for ad hoc networks in constrained situation", IEEE Int. Conf. Pers. Wirel. Commun. 2005. ICPWC, pp 86-89, 2005.
[8] R.Draves, J. Padhye, and B. Zill "Comparison of routing metrics for static multi-hop wireless networks", Conf. Appl. Technol. Archit. Protoc. Comput. Commun. – SIGCOMM, pp 133, 2004.
[9] Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," vol. 2, pp. 1–22, 2004.
[10] Kumar.et.al "Performance Comparison Of AODV and DSR Routing Protocols In MANET",2006.
[11] Ramanathan and M. Steenstrup, "A survey of routing techniques for mobile communications networks", Mob. Networks Appl, pp 89-104, vol. 1, no. 2, 1996.
[12] Zou, B. Ramamurthy, S. Magliveras, and B. Raton Routing Techniques in Wireless Ad Hoc Networks — Classification and Comparison.
[13] Hallani and S. Shahrestani, "Improving the Performance of Wireless Ad-hoc Networks: Accounting for the Behavior of Selfish Nodes", Commun. IBIMA, pp 1-11, 2011.
[14] Saraeian, F. Adibniya, M. Ghasemzadeh, and S. Abtahi, "Performance Evaluation of AODV Protocol under DDoS Attacks in MANET", pp 484–486, 2008.
[15] Charles E. Perkins, Elizabeth M. Royer and Samir R. Das and Mahesh K. Marina "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks" published in IEEE Personal Communications-February, pp. 16–28, 2001.
[16] Boukerche.A "Performance comparison and analysis of ad hoc routing algorithms", IEEE International Conference on Performance, Computing and Communications , pp. 171-178., April,2001.
[17] Baadache, and A. Belmehdi "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
[18] Jain, M. Jain, H. Kandwal "Advanced Algorithm for Detection and Prevention of Cooperative Black and Grayhole Attacks in Mobile Ad Hoc Networks", Intl. Journal of Computer Applications , Published by Foundation of Computer Science, 2010.
[19] Weerasinghe, H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation", Proc. of Intl. Conference on Future Generation Communication and Networking (FGCN'07) , pp 362-367, 2007.
[20] Cheung S, Lindqvist U, Fong M " Modeling multistep cyber attacks for scenario recognition.", In DARPA Information Survivability Conference and Exposition, pp 284–292, Vol. 1, 2003.
[21] Yang J, Ning P, Wang XS, et al, "CARDS: A distributed system for detecting coordinated attacks", Proc. of IFIP TC11 16th Annual Working Conference on Information Security, 2000.
[22] Hu, A. Perrig, and D. B. Johnson, " Rushing attacks and defense in wireless ad hoc network routing protocols", ACM Work, pp 30, 2003.
[23] Chen, S. Guo, K. Zheng, and Y. Yang, "Modeling of man-in-the-middle attack in the wireless networks", Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM pp 2255–2258, 2007.
[24] Davies "Evaluating Mobility Models Within An Ad Hoc Network", 2004.
[25] Kumar, S.A., Babu, E.S., Nagaraju, C. and Gopi, A.P., 2015. An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET. International Journal of Electrical and Computer Engineering, 5(5).
[26] P-C Tsou, C. J-M Chang, Y-H Lin, H-C Chao, J-L Chen, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", Feb. 13~16, Phoenix Park, Korea, 2011.
[27] B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multihop wireless ad hoc networks," in Ad Hoc Networking, C. E. Perkins, Ed. Reading, MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.
[28] [Online]. Available: http://www.isi.edu/nsnam/ns/
[29] 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.
[30] 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.
[31] 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.
[32] Gopi, A.P., Babu, E.S., Raju, C.N. and Kumar, S.A., 2015. Designing an Adversarial Model Against Reactive and Proactive Routing Protocols in MANETS: A Comparative Performance Study. International Journal of Electrical and Computer Engineering, 5(5).
[33] Babu, E.S., Rao, P.S., Rao, M.S. and Nagaraju, C., Quantitative Performance Evaluation of DSDV and OLSR Routing Protocols in Wireless Ad-hoc Networks.

Authors' Profiles

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 12 years of teaching experience. He has published 8 research papers in various International Journal and 30 research papers in various National and International Conferences. He has attended 32 seminars and workshops. His areas of interests are wireless communication and MANETs, Security, Mobile Sensor Networks.

Dr. C. Naga Raju received his B.Tech degree in Computer Science from J.N.T.University Anantapur, M.Tech degree in Computer Science from J.N.T.University Hyderabad and PhD in digital Image processing from J.N.T.University Hyderabad. Currently, he is working as an Associate professor in YSR College of Engineering of YV University, Poddutur. He has 16 years of teaching experience. He has published 100+ research papers in various National and International Journals and about 50+ 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.

Dr. MHM. Krishna Prasad received his B.Tech from CBIT Hyderabad, M.Tech degree in Computer Science from J.N.T. University Hyderabad and PhD in Computer Science & Engineering from J.N.T. University Hyderabad. Currently, he is working as a professor in the Dept. of CSE JNTUK University College of Engineering JNTUK, Kakinada. He has 20 years of teaching experience. He has published 50 research papers in various National and International Journals and various research papers in National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.

How to cite this paper: E.Suresh Babu, C. Nagaraju, MHM Krishna Prasad,"Empirical Performance Evaluation of Reactive Routing Protocols for Wireless Ad hoc Networks in Adversarial Environment", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.8, pp.47-58, 2016.DOI: 10.5815/ijcnis.2016.08.06

