ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 1, pp: (8-17), Month: January-March 2014, Available at: www.researchpublish.com

A Novel Approach to Security in Mobile Ad Hoc Networks (MANETs)

[1]Abu Taha Zamani, [2]Javed Ahmad

[1]Lecturer, Deanship of Information Technology, Northern Border University, Kingdom of Saudi Arabia
[2]Lecturer, Department of Computer Science Jazan University, Jazan, Kingdom of Saudi Arabia

***Abstract*: Ad hoc networks provide flexible and adaptive networks with no fixed infrastructure and dynamic topology. Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network. MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Mobile ad-hoc network is a group of two or more devices or nodes with the capability of communication and networking. It is an infrastructure less network. Such network may operate by them or may be connected to a larger internet. Due to its mobility and self-routing capability nature, there are many weaknesses in its security. The security of the network from various attacks is an important issue in MANET application now days. Due to the dynamically changing topology, open environment and lack of centralized security infrastructure, a mobile ad hoc network (MANET) is vulnerable to many attacks. This paper focuses on mobile ad hoc network's routing vulnerability and analyzes the network performance under Distributed Denial of Service MANETS.**

***Keywords*: Ad hoc Routing Protocols, AODV, DSDV, DSR, MANETs, Security attacks.**

I. INTRODUCTION

MANETs are formed by mobile nodes communicating with each other through wireless links without any governing body. These mobile nodes can be Personal Digital Assistants (PDAs), laptops, cell phones that communicate with each other without any fixed infrastructure and central management. Such networks can be used in the battlefield application, in disaster management and in remote areas where establishment and management of fixed network is not possible. These can also be used in the areas where the establishment of fixed infrastructure is very difficult. MANETs can also be used to deploy and coordinate the drones in the battlefield. They are characterized by unreliable communication media where the network topologies change dynamically. Additionally each node is limited by bandwidth, battery and computation power.

Due to the self-configuring nature of networks and lack of infrastructure, the nodes in the MANETs act both as a router as well as a host. As MANETs are self-developing and highly dynamic, some special ad-hoc routing protocols have been developed. Ad hoc routing protocols should have the following properties:

Distributed Operation: The protocol should be distributed. It should not be dependent on any centralized authority. This is beneficial because the nodes can enter and leave the network easily.

Loop Free: For the efficient functioning of the network, the routing protocol should guarantee that the routes are loop free. This avoids the wastage of bandwidth and computing power. Also, delays are reduced if the routes are loop free.

Demand based Operation: To avoid the unnecessary wastage of bandwidth, computing power and battery, the routing protocol should react only when necessary. In other words, the protocol should be reactive.

Unidirectional Link Support: Unidirectional links are formed in the radio environment. The protocol should use these unidirectional links for the optimal performance of the protocols.

Security: Security is an important issue in MANETs. MANETs are susceptible to attacks like spoofing. To guarantee the desired behavior in ad hoc routing protocols some security measures are required. Security can be improved by applying encryption and authentication to the routing protocols.

Quality of Service Support: Quality of Service is an important parameter in the ad hoc routing protocols. The routing protocols should support various QoS. For instance, real time traffic should have low jitter. It should be noted that none of the proposed protocols have all these properties.

Multiple routes: The protocol should have redundant routes, so when one link fails an alternative route can be used without initiating route discovery. Also, buffering multiple routes makes the protocol resistant to frequent topology changes.

Power conservation: The nodes that form the ad hoc network have very limited resources. One such important resource which is limited is the battery power. The protocols should conserve the battery power of the mobile devices. They should switch to power saving or standby mode when not in use.

Some of the commonly used ad hoc routing protocols in MANETs are Destination-Sequenced Distance Vector (DSDV) [1] routing, Dynamic Source Routing (DSR) [1], [2], Ad-hoc On-demand Distance Vector (AODV) routing [6], Optimized Link State Routing (OLSR) [58] and Zone Routing Protocol (ZRP) [6]. A brief summary of these ad hoc protocols is presented below.

Summary of different Ad-hoc Routing Protocols

- Divecha et al. [1] have carried out the performance analysis of DSDV and DSR protocols and compared their performances with different mobility models. They concluded that the routing protocols are specific to particular mobility models.
- Ramesh et al. [2] have proposed a method to reduce the end to end delay in the multi-path routing protocol by proposing a congestion aware multi-path DSR protocol. It enhances the performance of DSR protocol in congested network. The proposed protocol was compared with ordinary DSR protocol and the results show that the proposed scheme greatly reduces the end to end delay and improves the overhead.
- Williams and Camp [3] have presented a comprehensive comparison between different broadcasting schemes used in MANETs. In their paper, they categorized different broadcasting schemes and compared them through simulations, which established various network failures under different conditions like bandwidth consumption, dynamic topologies, and battery consumption. They have also proposed some protocols extension that can adapt to the changing network conditions and improve the functioning of the broadcasting scheme.
- Adibi and Agnew [4] in their paper presented a survey on different versions of DSR, pointed out their differences and compared them. The authors have also proposed a multilayer flavored DSR protocol which obtains the information from physical, MAC and network layer and passes this information to the network layer. Then they

select the most optimal routing protocol by performing a comparison between the current network condition and the pre-defined closest group of conditions.

- Toubiana et al. [5] performed a comparison of different multipath reactive routing protocols. The authors have compared three node-disjoint multipath routing protocols and two routing protocols based on an Untrusted Node Disjoint (UND) path scheme. The comparison showed that the multipath scheme limited the exerted performance degradation compared to UND. The comparison also showed that the multipath scheme incurred more overhead in the safe and secured network.
- Mittal and Kaur [6] compared the performance of DSR, AODV and ZRP protocols. The comparison was performed on various metric and the results show that AODV performed the best in achieving the end to end delay and packet delivery ratio while DSR performed the best with minimum number of hops in comparing TTL based hop count.
- Gowrishankar et al. [58] compared the performance of AODV and OLSR protocols. For a network with static traffic and smaller number of nodes, AODV performs well as it uses fewer amounts of resources. OLSR shows higher efficiency in networks where the node density is high and the traffic pattern is random.

This paper is organized as follows: Section 2 explains some of the common security threats and vulnerabilities in MANETs. Section 3 presents the techniques to mitigate the security threats in MANETs. Section 4 gives the Comparative Analysis of the techniques discussed in Section 3. Section 5 draws the conclusion of this paper.

2. SECURITY THREATS AND VULNERABILITIES IN MANETS

Due to the inherent property of the MANETs of being structure-less, dynamic, self-configuring and self-sustaining in nature, there exist some potential loopholes and vulnerabilities in MANETs that can be attacked and exploited by the malicious and undesirable nodes to disrupt the smooth functioning in the network. Some of the common attacks in MANETs are:

Impersonation or Spoofing

The objective of this attack is to hide the real identity of the attacker. In this attack, the attacker assumes the identity of a more trusted node in the network. By doing this the other nodes include this malicious node in their routing path and the malicious node can then disrupt the normal functioning of the network without being noticed.

Black-hole Attack

The purpose of this attack is to increase the congestion in network. In this attack the malicious node does not forward any packets forwarded to it, instead drops them all. Due to this attack the packets forwarded by the nodes do not reach their intended destination and the congestion in the network escalates due to retransmissions.

Sink-hole Attack

The idea of the attacker in this attack is to attract all the network traffic towards itself. The attacker executes this attack by making the neighboring nodes believe that the shortest path to the destination is through it. This attack causes the other nodes to relay all the traffic through the malicious node so that the attacker can modify, fabricate or just listen to the received packets.

Wormhole Attack

The main aim of the wormhole attack is to replay the packet on the other side of the network. This attack is executed by two nodes colluding to form a wormhole. The attacker on one side make the nodes believe that distance to the destination is just one hop, when it is greater than one hop. This causes the attacker to attract all the traffic from one side of the network andrelay it through the wormhole; the attacker on the other side replays the same packet. By doing this the attacker can drop the packets or obtain any service illegally.

Sleep Deprivation

The goal of the attacker in this attack is to keep the target node constantly busy. This attack is initiated by flooding the network with routing traffic and thereby making the node consume all of the computing and battery power. This attack forces the targeted node in consuming the battery, network bandwidth and computing power by spurious requests for existent or non-existent destination nodes, so that it cannot process the legitimate requests.

Rushing Attack

The purpose of this attack is to include the malicious node in the routing path. During the route discovery phase the RREQs are forwarded by the malicious nodes to the neighbors of the target node. These RREQs are quick to reach the neighboring nodes. When a neighboring node receives this hurried RREQ from the attacker, it will not forward any request originated from the source node that initiated route discovery. By executing this attack the attacker includes itself in the routing table and can then tamper with the packet.

Location Disclosure

The location disclosure attack intends to target the privacy requirements of the ad-hoc network. In this attack the attacker, by doing traffic analysis or using simple monitoring, approaches and finds the location of the destination node in the network. By knowing the intermediary nodes the attacker can find the node of concern and gain the information about the structure and the topology of the network.

Routing Table Poisoning

The intention of the attacker in this attack is to corrupt the routing table. The routing protocols maintain the routing tables to find a route to the destination and forward the packet to the anticipated node. In this attack, the malicious nodes generate and send the fabricated traffic into the network or modify the legitimate messages from other nodes. An alternative way to execute this attack is by broadcasting a RREQ with higher sequence number in the network resulting in the valid packets with lower sequence number to get rejected. This attack causes the routing tables to create wrong entries and store the corrupt invalid information in the routing tables of the participating nodes.

Route Fabrication

The objective of this attack is to gain illegal access to the packets or to initiate packet dropping in network. In this attack, an attacker hinders with the normal routing procedures. This attack is executed by changing the routing messages or by inserting false routing messages. Due to the fabrication of routing information the packets are routed to non-existent nodes or they can be forwarded to a malicious node. It also results in the delay of the packets and bandwidth wastage. Routing fabrication also leads to Denial of Service (DoS) attacks.

Denial Of Service (DoS) Attack and Flooding

The aim of this attack is to cripple the smooth functioning of the network. This attack is accomplished by continually sending packets into the network causing the targeted node in the network to process them and keep them occupied resulting in the crashing of that node. By executing this attack, the attacker keeps the targeted node busy in processing its fabricated packets and depriving the legitimate RREQs to be dropped. This attack can cause the network infrastructure to collapse.

Routing Table Overflow

The principle of this attack is to consume the routing table buffer. The attacker sends false and engineered traffic into the network. It modifies the packets and includes the routes to non-existent nodes. This attack overwhelms the routing table buffer by storing false routing information in the routing table. This blocks the processing of legitimate routes and storing them since the routing table runs out of space. This kind of attack can be particularly executed and severely affect the DSR protocol as it stores the route to every node resulting in the exhaustion of the route cache.

3. TECHNIQUES TO MITIGATE VARIOUS SECURITY ATTACKS IN MANETS

In this section we will be presenting a survey on different techniques that are proposed to enhance and fortify the ad hoc routing protocols against various security loopholes and vulnerabilities in the ad hoc networks.

3.1 Solution Using Trust Values

In this subsection, various trust value based solutions have been discussed. These solutions mitigate various security vulnerabilities and enhance the existing ad hoc routing protocols.

Pirzada and McDonald [7] present a method to improve the DSR protocol. They propose the method of deploying trust gateways to reinforce the DSR protocol. In this method, the number of malicious nodes in the network is identified and with the use of the trust gateways, they are avoided in the future exchange of data packets.

In the Trusted Dynamic Source Routing [8] model by Yong et al., trust among nodes is calculated using a combination of direct and indirect trust. When the trust value of a node declines so much that it falls below a threshold, it is then added to a blacklist. The packets from the blacklisted nodes are not forwarded.

Dhurandher and Mehra [9] have employed a message trust based solution to the multipath routing scenario. In this proposed solution each node is initially given a zero trust value indicating an unknown trust level. Based on the behavior of the nodes the assigned trust value is either incremented or decremented. Trust values may be positive,negative or zero, indicating known, malicious, or unknown behavior.

3.2 Wormhole Detection Method

This section presents the solution to prevent and detect wormhole in ad hoc networks.

Lee et al. have proposed a solution to mitigate the wormhole attack in MANETs [18]. Here the wormhole is collectively detected by route identification. Each node maintains its neighbor’s information, thus identifying the route that is suffering from the wormhole. Sharma and Trivedi [19] proposed a method to defend against the wormhole attack. In the proposed solution the authors use digital signatures to prevent against the wormhole attack. Whenever a node wants to send a packet it initiates RREQ. Along with RREQ it also sends its digital signature. The nodes in the network verify this digital signature with the one stored in their database and if there is match, they confirm that the RREQ is from a legitimate source. The malicious node replaying the RREQ either has a signature of other node or does not have any and hence is identified and isolated from further transmission.

3.3 Intrusion Detection Systems (IDS)

This section provides different Intrusion Detection and Prevention Systems.

Negar et al. proposed an Intrusion Detection System (IDS) [20] based on the interaction between the user and the kernel processes. A feature list is created to distinguish between the normal and anomalous behavior. They introduce a new function to the Linux Kernel called the Wrapper Module to log initial data to prepare the intended feature list. For the classification of the input vectors SVM neural network is applied in the proposed scheme. The authors tried to improve the accuracy, training time and testing time as compared to other systems. Wei and Wu [21] present a method that combines feature extraction and SVM (Support Vector Machine) model to improve the classification accuracy and minimize the detection time. In the feature extraction using CEGA (Classification Ensemble by Genetic Algorithms), the fitness of the individual is calculated by classification rate and conditional entropy. The SVM model on the other hand is processed simultaneously that finds the optimal feature subset. The proposed method is effective in intrusion detection. Visumathi and Shunmuganathan [22] proposed architecture for Intrusion Detection System that uses SVM classifiers. The authors presented a survey of the existing intrusion detection systems.Penvaand and Bringas [23] proposed a method that detects the misuse and the anomalies in the network. The authors use Bayesian networks to learn the misuse and anomalies and use this knowledge to further detect other known and unknown attacks.

3.4 Black-hole detection and prevention

This section presents the solution to black-hole detection and prevention method.

Wang and Shi [43] proposed a scheme to secure DSR protocol based on request sequence number. The scheme uses creditable routing information which is formed and based on the acknowledgements received by the source from the destination. The information of the routing table is centered on the source node of the RREQ and is divided according to the trust value which in turn decides the routing path of the RREQ packets. This ensures that every node has valid information and black-hole attack can be prevented. Cai et al. [44] introduced a method to detect black-hole and gray-hole attacks in ad hoc network. The authors have proposed a path-based method that overhears the next hop's actions. As the scheme does not send out control messages it saves the system resources. To lower the false positive rate under high network overload, a collision rate reporting system is established in the MAC layer. This adaptive threshold approach decreases the false positive rates.

3.5 Sink-hole Detection and Prevention Method

Culpepper and Tseng [47] have introduced Sinkhole detection system to combat sink-hole in DSR protocol. In this system there are three variables: Sequence Number Discontinuity, Previous Image Ratio and Route Add Ratio. All these three variables tell if there is a sinkhole present in the network and if their values are high, low and high as compared to a predetermined value. Sheela et al. [48] have presented a method to defend against the sink-hole attack in wireless sensor networks. In the proposed method the authors use what they call as the mobile agent programs. These agents travel to each and every node in the ad hoc network, collect the information and update the routing table of the nodes with the latest information. This mechanism causes every node to be aware of all other nodes in the network and this allows it to ignore the bogus information from the malicious node, trying to launch the sink-hole attack.

3.6 Credibility Management and Routing Test

Pengwei and Zhenqiang [50] have proposed a method that enhances the security of the AODV protocol. In this proposed method the authors enhance the security of the AODV by declaring a neighbor table. This neighbor table contains three fields: the neighbor IP, expired time and Credit value. Initially, the credit value of the node is set to 1. When a node sends the data packet in the network it stores a copy of that packet in its buffer. Then, when other nodes rebroadcast the packet and if the listened packet is same as the packet stored in the buffer of the listening node's buffer, it increments the credit value of the neighboring node in the neighbor buffer table, otherwise decrements the credit value by some factor.

3.7 Link Cache Updating

DSR protocol maintains cache to keep the redundant routes. Over time the routes in cache become stale. To avoid this problem Yu [51] proposed a scheme to update the cache and keep the fresh routing information. In the proposed method the author defines a cache table and defines a distributed cache algorithm. Necessary information for cache updates is stored by each node in its cache table. Whenever a link failure is detected in the network, the algorithm spreads this information to all the nodes in the network link and updates their related cache table. This process is completed in a distributed manner. The proposed method does not depend on any ad hoc parameters of the network and hence is fully adaptive to the topology changes.

3.8 Flooding Attack Prevention Technique

Different solutions to prevent the Flooding Denial of Service (DoS) attack have been discussed in this section.

Kataria et al. [52] have proposed a scheme to control the flooding of fake route requests in ad-hoc networks. To control the flooding of fake route requests and to ensure fairness to genuine RREQs, a parameter known as RREQ_RATELIMIT is considered, it is fairly distributed among all the participating nodes. This limited bandwidth which is allotted to each node restricts the number of RREQs injected in the network and processed by each node. Jia et al. [53] proposed a method to prevent the Denial of Service (DoS) attack in multi-path communication in Mobile Ad hoc Networks (MANETs). A capability message has been defined that is exchanged by each node. This enables them to maintain a global view of the overall throughput of the flow in the network and dynamically adjust to local constraints to prevent a DoS attack. The presented method alleviates DOS attack by regulating the end to end traffic transmitted over the network.

3.9 Data Hiding Technique

Dey et al. [56] introduced a data hiding technique. This technique is based on the decomposition of number in sum of prime numbers. This generates a different set of bit-planes which is suitable for embedding. This enables embedding of secret messages in higher bit planes without causing any distortion. A better stego-image quality is achieved in reliable and secured manner, guaranteeing efficient retrieval of data. A comparison between the classical Least Significant Bit (LSB) method, the Fibonacci LSB data-hiding technique and the proposed scheme was carried. It was observed that stego-image hidden was indistinguishable from the original cover-image. This idea can be extended to increase security in ad hoc networks.

3.10 First Fast Second Reliable Method (FFSR)

Zhai et al. [57] have presented a method that improves the reliability and efficiency of AODV protocol. In this paper, they propose an idea called “First Fast Second Reliable (FFSR)” that ensures the transfer of data packages in the shortest and the most reliable mode. The routing metric in this method is based on the cognition of each node and all the nodes in cognitive ad hoc network collect information about the whole network periodically.

3.11 Multi-Factor Authentication Techniques

In [59], [60] authors have proposed a Multi-factor security authentication method for wireless payment. This idea can very easily be extended to provide better security in ad hoc networks protocol. In [61] this technique has been used to prevent impersonation in ad hoc networks.

4. COMPARATIVE ANALYSIS OF DIFFERENT TECHNIQUES

In this section we provide a quantitative comparison between the different techniques discussed in the previous section to mitigate various attacks.

4.1 Detection of Malicious Nodes on Trust Value Technique

In this subsection, we compare different trust value techniques to detect and avoid the malicious nodes. The solution proposed in [7] uses Trust Gateways to identify the malicious nodes whereas the method proposed in [8] employs direct and indirect trust as compared to simple Trust Gateways discussed earlier. The advantage of this method is that it maintains a blacklist that contains the list of misbehaved nodes. The nodes from this list are excluded while forming the routing information. The method proposed in [9] uses positive, negative and zero trust values to identify the known, malicious or unknown behavior of the nodes in the network. The technique proposed by [12] employs a rather different solution to calculate and assess the trust values. It uses fuzzy logic to establish the trust levels of the node. The scheme suggested in [13] employs watchdog and path rater concept. In this method the watchdog detects the misbehaving nodes and the path rater makes sure that these nodes are not included in the forwarding routes. From simulations results, it has been observed that this protocol performs normally even when a large percentage of the nodes in the network are malicious.

From the above comparison of various trust based techniques we infer that the trust values are utilized to detect the malicious nodes in the network thereby avoiding them and selecting optimal communication path.

4.2 Comparison of techniques to mitigate Wormhole attack

This subsection compares various techniques to detect and prevent the wormhole attack.

The method proposed in [18] employs a cooperative method to detect a wormhole. Each node in this scheme maintains its neighbor’s information. This technique detects the wormhole attack in the network. On the other hand the technique suggested in [19] uses digital signatures to prevent the wormhole attack. Each node, when receiving the RREQ, cross-checks the digital signature in the packet with the one stored in its routing table. If it is legitimate then it forwards the packet otherwise it informs other nodes that the previous node that forwarded the packet is a malicious node, thus preventing the wormhole attack.

4.3 Comparison of different IDS Techniques

We compare different IDS techniques discussed in the previous section.

The solutions proposed in [20], [21], [22] use SVM model to design Intrusion Detection System. The method suggested in [20] uses a wrapper module along with SVM network to improve the accuracy, testing time of the IDS. On the other hand CEGA [21] is employed together with SVM model to make the IDS system more effective. The solution proposed in [22] employs plain SVM classifiers in the architecture of the IDS system. A different method is suggested in [23]. Bayesian networks are used, that learn from the misuse of the network and the anomalies and detects other known and unknown attacks.

4.4 Comparison of different Black-hole detection Methods

In this subsection we provide the comparison of various techniques discussed in the preceding section.

The method suggested in [44] uses path based approach that overhears the next hop’s actions. This scheme does not send out control messages thus reducing the overhead. On the other hand, the technique proposed in [46] verifies the control messages sent by the intruder. A two-fold scheme [45] is employed that prevents the black-hole attack. In this scheme the acknowledgements are sent to the source by the nodes when they receive the packet. When the source does not receive the acknowledgment, it infers that a malicious node is present in the network.

4.5 Comparison of Sinkhole Detection Methods

In this subsection we compare the various techniques discussed to mitigate sinkhole detection attack.

In [47] a sinkhole detection scheme is presented. In this scheme three variables are used that detect if sinkhole is present in the network or not. Alternatively, mobile agents [48] are used in wireless sensor networks to detect the sinkhole. In this method the mobile agents travel to each node collecting the information and making each node aware of others, thus preventing the sinkhole attack. A trust-based method [50] is used that compares with a predefined threshold to detect the sinkhole.

4.6 Comparison of techniques to prevent the Flooding Attack

Here we compare various techniques that are applied to prevent the flooding attack.

In [52] a parameter known as RREQ_RATELIMIT is used to put a limit on the number of RREQs introduced in the network. This prevents the flooding of RREQs. A solution presented in [54] delays the RREPs in the network so that the source does not get overwhelmed with unnecessary RREPs, thus preventing the flooding attack. A different approach is chosen in [55] as compared to the earlier schemes in [52] and [53]. In this method phase transition phenomenon, discussed in percolation and random graphs, is used to define the probabilistic flooding algorithm.

5. CONCLUSION

In this paper we surveyed various protocols for MANETs, discussed various security vulnerabilities to mitigate the attacks and presented the performance analysis of several routing protocols.In the Introduction section we discussed about MANETs, listed their advantages and how they are formed. We also discussed different ad hoc routing protocols, explained the working of each and provided a table that lists the ad hoc routing protocols and the properties exhibited by each of them. In the next section we listed various security vulnerabilities and threats that are encountered in the MANETs. We explained each of the security threats and the effects they cause on the ad hoc networks. In the last section we discussed several techniques to mitigate the security threats and attacks listed in the previous section. We categorized the solutions based on various techniques. We also provided a comparative analysis of different techniques that are employed to mitigate diverse security issues and presented a table that summarizes the entire section 4.

REFERENCES

[1] Bhavyesh Divecha, Ajith Abraham, Crina Grosan. Sugata Sanyal, “Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models”, *First Asia International Conference on Modeling and Simulation*, AMS2007. March, 27-30, 2007, Phuket, Thailand. Publisher: IEEE Press, pp. 224-229.

[2] V. Ramesh, P. Subbaiah, N. Sandeep Chaitanya, K. Sangeetha Supriya, “Performance Comparison of Congestion Aware Multi-Path Routing (with Load Balancing) and Ordinary DSR”, *2010 IEEE 4th International Conference on Internet Multimedia Services Architecture and Application(IMSAA),*Dec. 15-17, 2010, pp.1-5.

[3] Brad Williams, Tracy Camp, “Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks”, *MOBIHOC’02,* June 9-11, 2002, EPFL, Lausanne, Switzerland, pp. 194-205.

[4] S. Adibi, G.B. Agnew, “Multi-layer flavored dynamic source routing in mobile ad-hoc networks”, *IET Communications*, 2008, Vol. 2, No. 5, pp. 690–707.

[5] Vincent Toubiana, Houda Labiod, Laurent Reynaud and Yvon Gourhant, “Performance Comparison of Multipath Reactive Ad hoc Routing Protocols”, *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008),* Sept. 15-18, 2008,pp.1-6.

[6] Shaily Mittal, Prabhjot Kaur, “Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANETS”, *International Conference on, Advances in Computing, Control, and Telecommunication Technologies, 2009. ACT '09*, Dec. 28-29, 2009, pp.165-168.

[7] Asad Amir Pirzada, Chris McDonald, “Deploying Trust Gateways to Reinforce Dynamic Source Routing”, *2005 3rd IEEE International Conference on Industrial Informatics, (INDIN '05),*Aug. 10-12, 2005, pp. 779- 784.

[8] CHENG Yong, HUANG Chuanhe, SHI Wenming, “Trusted Dynamic Source Routing Protocol”, *Wireless Communications, International Conference on Networking and Mobile Computing, WiCom2007*, Sept. 21-25 ,2007,pp.1632-1636.

[9] Sanjay K. Dhurandher, VijetaMehra, “Multi-path and Message Trust-Based Secure Routing in Ad Hoc Networks”, *International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT '09.*, Dec. 28-29,2009, pp.189-194.

[10] R. S. Mangrulkar, Mohammad Atique, “Trust Based Secured Ad hoc on Demand Distance Vector Routing Protocol for Mobile Ad Hoc Network”, *2010 Sixth International Conference on Wireless Communication and Sensor Networks (WCSN),* Dec. 15-19 ,2010,pp.1-4.

[11] H. Hallani, S.A. Shahrestani, “Trust Assessment in Wireless Ad-hoc Networks”, *Wireless Days, 2008 (WD '08). 1st IFIP, Dubai,* Nov. 24-27, 2008,pp.1-5.

[12] JaydipSen, “A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks”, *Proceedings of the 3rd International Conference on Network Security and Applications*, Chennai, India, 2010, pp. 538- 537.

[13] Sonja Buchegger, Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)”, *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC’02),* June 9-11, 2002, EPFL Lausanne, Switzerland, pp. 226-236.

[14] Islam Tharwat A. Halim, Hossam M. Fahmy, Ayman, M. Bahaa El-Din, Mohamed H. El-Shafey, “Agent-based Trusted On-Demand Routing Protocol for Mobile Ad-hoc Networks”, *2010 4th International Conference on Network and System Security (NSS)*Sept. 1-3, 2010, pp. 255-262.

[15] Edith C.H. Ngai, Michael R. Lyu, “Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks”, *Proceedings of 24th International Conference on Distributed Computing Systems Workshops, 2004*, March 23-24, 2004, pp. 582- 587.

[16] Ming Yu, Mengchu Zhou, Wei Sou, “A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments”, *IEEE Transactions on Vehicular Technology*, vol.58, no.1, Jan.2009, pp.449-460.

[17] R. Vasudevan, Sugata Sanyal, “A Novel Multipath Approach to Security in Mobile and Ad Hoc Networks (MANETs)”, *Proceedings of International Conference on Computers and Devices for Communication (CODEC'04)*, Kolkata, India, December, 2004, pp. CAN_0412_CO_F_1 to CAN_0412_CO_F_4.