Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Technique to Detect and Isolate Replay Attack in ALARM Protocol

Gagandeep Kaur Virk
Department of CSE
GZS PTU Campus, India

Dinesh Kumar
Department of CSE
GZS PTU Campus, India

Abstract— MANET (Mobile Ad hoc Network) is the self configuring type of network in which mobile nodes can join or leave the network when they want; it is a decentralized type of network. Due to these unique properties of the MANET, it is much vulnerable to security attacks. ALARM protocol (Anonymous Location Aided Routing in MANET) is used in MANET to achieve the key security objectives, i.e. confidentiality, authentication, authorization, integrity. ALARM protocol is based on certain assumptions, such as, location of the mobile nodes, time at each node, range of mobile nodes etc. According to time assumption, clocks of the mobile nodes are weakly synchronized. Due to weak clock synchronization assumption, there is a possibility of replay attack in the network. In this work, novel technique has been proposed to detect and isolate replay attack in ALARM protocol. The proposed technique is based on ICMP (Internet Control Message Protocol) message and simulation results show that this technique performs well under fixed network conditions.

Keywords— ALARM, ICMP, MANET, Privacy, Replay attacks, Synchronization.

I. INTRODUCTION

Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols wirelessly. It can be either infrastructure or infrastructure-less. In infrastructure based network, communication takes place only between the wireless nodes and the access points. In infrastructure-less network, there is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks. Ad-hoc network is an infrastructure-less network and thus decentralized type of wireless network. In ad-hoc network, every node participates in routing by forwarding data to all the nodes in the network and then determining dynamically, on the basis of network connectivity, the nodes which forward data. Nodes within each other's radio range communicate directly while those which are not in each other's range communicate using other intermediate nodes. Ad-hoc network is a new standard of wireless communication for mobile hosts. Such networks are used in case of urgent situations. MANET (Mobile Ad-hoc Network) is one of the types of Ad-hoc network. Every device in MANET is free to move by itself in all the directions. It can change its links to other devices frequently. The main challenge in building a MANET is making each mobile device capable to maintain the information which is necessary to route the traffic.

The complexity and uniqueness of MANETs makes them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified into two categories- passive and active, depending on whether the normal operation of the network is disrupted or not. A passive attack obtains data exchanged in the network, without disturbing the communication operation. The passive attacks are difficult to detect. These attacks compromise the confidentiality of the data [9]. Examples of passive attacks are snooping, eavesdropping etc. The active attacks are those in which any data or information is inserted into the network so that information may harm the normal operation of the network. These involve fabricating messages, dropping or modifying packets, replaying packets. Examples of active attack are spoofing, impersonation etc.

Replay attacks are active attacks, in which an attacker instead of modifying packet's contents just replays stale packets to exploit battery power, bandwidth and computational constraint of mobile nodes [9]. They lead to congestion in the network and mystification among the routing nodes because of conflicting information, thus, delaying packet delivery and/or preventing them from reaching the destination.

In the absence of mutual authentication, there are several type of active and passive attacks possible, for example, replay attack, sniffing, snooping etc. In our proposed work, we try to prevent these Replay attacks by using mutual authentication based protocol called ALARM, using cryptographic mechanism of digital signatures for carrying timestamp and location information of nodes privately in the network and ICMP messages for monitoring the network.

The rest of the paper is organized as follows: Section II describes the related work followed by description of ALARM protocol in Section III. In Section IV & V, we presented our proposed technique and experimental results respectively. And Section VI is the conclusion.

II. RELATED WORK

There are many routing protocols that can be used in MANETs. But most of them do not focus on privacy, especially, tracking-resistance i.e. making nodes untraceable. If nodes become traceable by other nodes, privacy of the nodes is compromised and it may lead to occurrence of various attacks like eavesdropping, location fraud etc. In this research work, many privacy-preserving as well as non-preserving protocols like SRDP [31], Ariadne, and SEAD were studied [30]. Mainly, privacy preserving ALARM protocol and its variants were considered.

Karim El Defrawy, and Gene Tsudik (2011), present the ALARM protocol for mutual authentication. In this technique, the mobile node presents its secondary identity which helps the node to become untraceable by all the other nodes. In ALARM protocol, certain packets are exchanged for mutual authentication and messages are digitally signed. The digital signature approach leads to message integrity and confidentiality. They have considered Sybil and location fraud attacks possible in ALARM. Overhead and scalability of ALARM is also evaluated and shown that it performs close to other optimal protocol (like OLSR).

Caimu Tang and Dapeng Oliver Wu (2011), proposed an efficient authentication mechanism for low-power devices [2]. In the proposed scheme, the mobile station only needs to pass one packet for mutual authentication. Elliptic-curve-crypto system based Trust Delegation mechanism is used to generate group pass code for mobile station authentication. This proposed mechanism requires less computations and less message exchange as compared to other authentication schemes. They used the elliptic-curve-crypto system based trust delegation mechanism to generate group pass code for mobile station authentication [2]. With the use of this authentication mechanism many active and passive attacks were prevented including the denial of service attack. This purposed mechanism required less computations and less message exchange as compared to other authentication schemes.

Tushar Sharma et al. (2013), have proposed an enhanced Watchdog Intrusion Detection System to secure MANET. This watchdog mechanism is based on nodes watching their neighbourhood nodes to detect misbehaviours. The watching nodes are called Watchdog nodes. If a watchdog detects that a packet is not forwarded within a particular time or is altered by its neighbor, it declares the neighbor as misbehaving [3].

[4] Presents Hybrid Anonymous Location-Aided Routing Protocol for MANETs. This technique uses both proactive and reactive routing. The proactive method is applied for the nodes which are within the pre-defined radius and reactive method is applied for nodes which are outside the pre-defined radius [4]. When the source wants to communicate, it is done using some cryptographic technique using topology information. Simulation results show that the proposed technique reduces overhead and delay and increases accuracy.

Anonymous On-Demand Routing protocol for MANETs is used in [5]. They have considered two types of attackers- external global passive attacker (they can monitor all communications among all nodes in the network at all time) and cooperating node as an attacker i.e. they have assumed that every node that is part of the network is a potential attacker. Anonymous nature of the protocol lies in the goals of the proposed protocol. For Example- preventing a node from learning the destination of some message, preventing a node from determining whether another node is part of a path between two nodes. So, this protocol is based on reactive routing along with anonymity.

Proactive routing protocol based on Link State algorithm is used in [6]. This protocol is optimized in the sense that it reduces the size of information sent in the messages and number of retransmissions to flood these messages by using the concept of Multipoint Relays (MPR). OLSR protocol is preferred in dense networks and where the communication is assumed to occur frequently between large number of nodes.

In [7], comparison between two Link State algorithms namely OSPF and OLSR is done, for ad-hoc routing. They considered various parameters of ad-hoc networks like neighbourhood size of each node, overhead of retransmitting the link states, topology - change rate. This analysis is based on the assumptions that time is slotted and that mobile nodes are synchronized. In this work, it is shown that OSPF performs quite poorly in most cases as compared to OLSR and hence OLSR is best suited for ad-hoc environments.

Yixin Jiangand et al. (2006), proposed a mutual authentication and key exchange protocol [11]. This protocol has two highlighting features which are: identity-anonymity and session key renewal. This protocol provides secure roaming services to the legitimate user [11]. The proposed protocol consists of two phases: First phase provides mutual authentication using anonymous identity which hides the user's real identity when a legitimate user is roaming from the home agent to the visiting agent. This phase uses the temporal identity (TID) instead of the user's real identity [11]. The second phase performs the session key renewal which renews the key shared between the legitimate user and the serving agent.

Steven M. Bellowing and Michael Merritt (1991), discussed about Kerberos authentication protocol and its limitations [12]. The main limitation of Kerberos authentication protocol is large number of message exchange needed for successful authentication and this approach degrades the battery performance of the hand held devices. Second, disadvantage is of assumptions of the Kerberos authentication protocol because when environment changes, assumptions are needed to change for efficient working of protocol. Few attacks possible using this protocol are Replay attack, login spoofing, session key expose, password guessing etc.

Sushma Yalamanchi and K.V. Sambasiva Rao (2011), have proposed a two stage authentication scheme for wireless networks. They discussed that in wired networks, we can use the authentication protocol having large computations but in wireless networks we require less computation and energy efficient authentication protocol because in wireless networks the hand held devices are having limited battery and limited computational resources [13]. In this paper, they presented a two-stage authentication scheme for wireless networks that uses strong authentication in Stage 1 and a lightweight symmetric key based authentication in Stage 2. The cost of authentication in Stage 1 is distributed over N sessions, which reduces the overall cost of the scheme.

Y.C. Hu et al. (2002), have designed and evaluated SEAD (Secure Efficient Ad-hoc Distance vector) routing protocol which is based on Destination-Sequenced Distance-Vector routing protocol. Using this secure protocol, they prevented Denial-of-Service attacks in the network and shown the better performance of the network by testing the routing protocol in different scenarios.

III. ALARM PROTOCOL

ALARM protocol is *Anonymous Location-Aided Routing* in MANET. ALARM is a privacy-preserving and secure link-state based routing protocol [1]. It uses node's current location value from Location Announcement Message (LAM) to construct a secure MANET map. Location information has become progressively more available through small and cheap GPS receivers. This technique utilizes proactive mode of location based routing. ALARM provides both security and privacy features by providing node authentication, data integrity, anonymity, and un-traceability [1]. It also protects the network from some of the passive and active attacks.

Message Type = LAM
Current Location (8 bytes)
Current Time Stamp (4 bytes) (TS)
Temporary-Cryptographic-Key (128 bytes) (PK-TMP)
Public-Key-Signature (250 bytes)
Group Signature (Location ‖TS ‖ PK-Tmp) (200 bytes)

Fig 1: Location Announcement Message

A. *Basic steps in ALARM's operation*

1) Initialization (Offline)

- The group manager (GM) starts with the basic group signature scheme and admits all legal nodes as group members. During this phase, each node member creates an inimitable private key that is not exposed to anyone. This key is desirable to produce valid group signatures [1]. It also generates a corresponding public key (PK member), that is exposed only to the GM. GM takes care of any contested group signatures by opening them and determining the actual signers.
- Based upon the specific group signature, GM might also hold joining of new members as well as revocation of the existing members. Revocation might not be feasible or desired.

2) Operation (Online)

- Time is divided into equal slots of duration T. At the beginning of each slot, each node s generates a temporary public-private key-pair PK-TMP (public) and SK-TMP (private), respectively [1].
- Each node broadcasts a Location Announcement Message (LAM), containing its location, time-stamp, temporary public key (PK-TMPs), and a group signature computed over these fields [1].
- When a node receives a new LAM, it first checks that it has not received the same LAM before. After that it checks the time-stamp and group signature to verify if they are valid. Then node rebroadcasts the LAM to its neighbors if both are valid. Temporary pseudonym is used to locate the node in the interval between two successive LAMs. The pseudonym includes temporary location of the node and group signature of the last Location Announcement Message. Including location in the pseudonym speeds up the forwarding process and requires less look-ups [1].
- Whenever the communication is needed, the node checks to see if any node currently exists at (or near) that location. If it is so, the node sends the message to destination and this message is encrypted with a session key using a symmetric cipher like AES. The session key is, in turn, encrypted under the current public key (PK-TMP) included in the destination's latest LAM [1]. When the destination receives the message, it first reacquires the session key and uses it to decrypt the rest. ALARM is not bound to any specific public key technique. However, Diffie-Hellman half-key is good choice.

- Forwarding: Message forwarding is not dependent on topology propagation. The path can be computed using the shortest path algorithm or any other location-aided routing algorithm, such as Convex Hull, GeoCasting etc [1].

B. *Assumptions and Goals of ALARM*

1) The following assumptions are necessary in ALARM:

- *Location:* Each node is provided with device that gives accurate positioning information of the node. Eg- GPS.
- *Mobility:* A certain minimum number of nodes move periodically such that group manager of new group extracts all the previous information about the node.
- *Time:* All nodes maintain weakly synchronized clocks.
- *Range:* Nodes have uniform transmission range. Once a node knows the present MANET map, it can determine node connectivity [1].

2) ALARM has the following goals:

- *Privacy:* There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations cannot be linked [1].
- *Performance:* Security and privacy goals must be achieved without affecting the performance.
- *Security:* The network must be resistant to passive and active attacks occurring from both outsider and insider malicious nodes [1].

IV. PROPOSED TECHNIQUE

In MANET, inside and outside attacks are possible, which degrade the network performance. To prevent these attacks, a trust relationship must be developed in the network among the mobile nodes. There are basically three assumptions in ALARM protocol i.e. mobility range, location and time. In time assumption, clock of mobile nodes are weakly synchronized due to weak clock synchronization of the mobile nodes. Due to this, replay attack is possible in the network and it reduces reliable data transmission between mobile nodes.

In this paper, a novel technique has been proposed to detect and isolate replay attack in mutual authentication based ALARM protocol. The optimal path is selected between source and destination using AODV protocol. The trust relationship is maintained between source and destination using ALARM protocol.

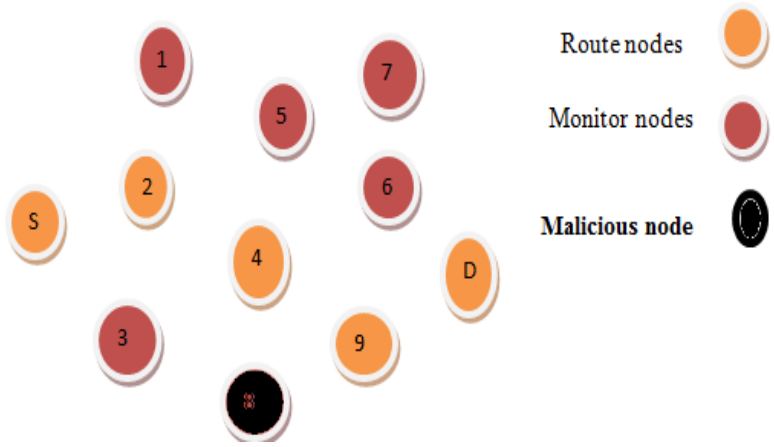

Fig 2: Activation of Monitor modes

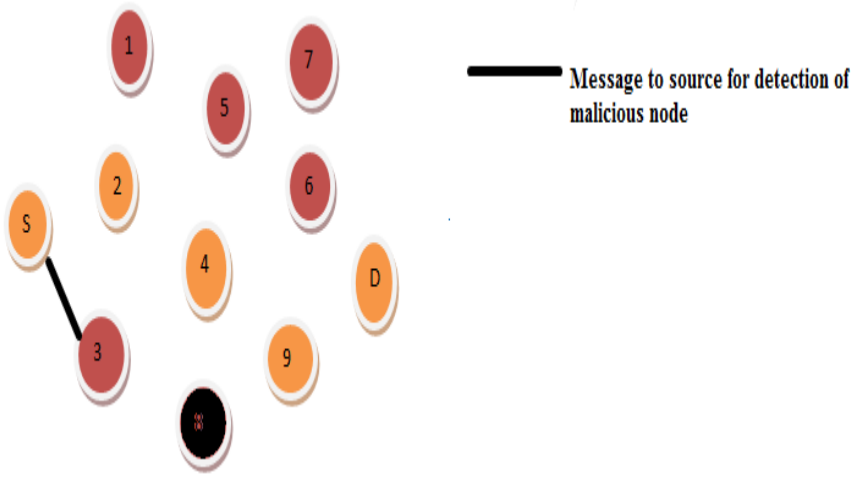

Fig 3: Detection of malicious node

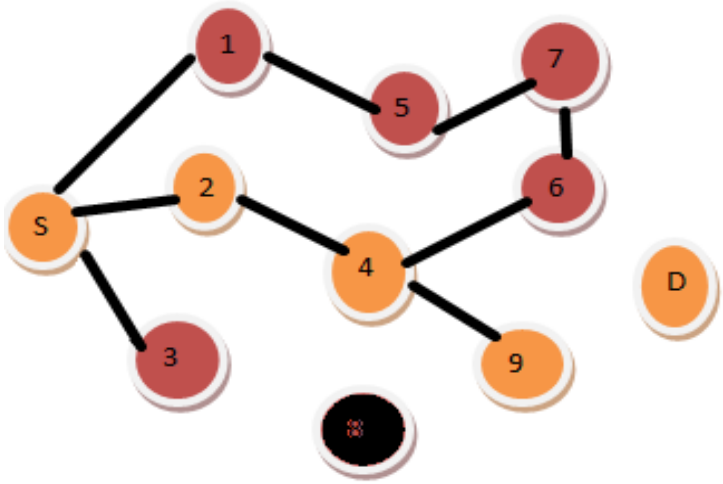

Fig 4: Isolation of malicious node

To test the route, source starts sending fake packets through a path. At that time, source also sends ICMP (Internet Control Message Protocol) packets to all other nodes. Nodes which receive ICMP packets go to Monitor Mode (as illustrated in Fig 4.1) to check whether its adjacent node is forwarding data packets within threshold time period or not. If not, then its adjacent will be detected as a malicious node. When the adjacent node is detected as malicious, monitoring node will send an information message to the source (as illustrated in Fig 4.2). On receiving the malicious node information, the source node will isolate the selected path as shown in Fig 4.3 and will select the second best path to the destination.

V. EXPERIMENTAL RESULTS

The proposed technique was implemented in NS2 (Network Simulator2) in two phases- Problem implementation and Solution implementation. In the first phase, simple communication between source and destination was implemented, using AODV on the basis of assumptions of ALARM. We analysed the communication pattern after path establishment between source and destination. It was noticed that there was large delay and packet loss due to the presence of malicious nodes in the network. In the second phase, solution for the above problem was implemented by using ICMP messages. Hence, after isolating the malicious node using novel technique, packet loss and delay were reduced dramatically.

Parameter	Value
No. of mobile nodes	17 for problem implementation, 19 for solution implementation
Routing Protocol	AODV
Plot area	800 x 800
Channel type	Wireless
Radio Propagation Model	Two-Ray
Antenna type	Omni-Directional
Interface queue type	Priority Queue
MAC type	802.11

Table 1: Simulation Parameters

In Fig 5, red line represents more packet loss due to replay attack and green line represents less packet loss due to selection of new optimal path after isolating replay attack (malicious node). This graph shows that new proposed technique has less packet loss as compared to old technique i.e- without ICMP message. Fig 6 depicts that delay is reduced in our proposed technique by isolating the malicious node immediately. In Fig 7, red line represents lesser throughput and green line represents new throughput. This graph concludes that new proposed technique increases the throughput of the network.

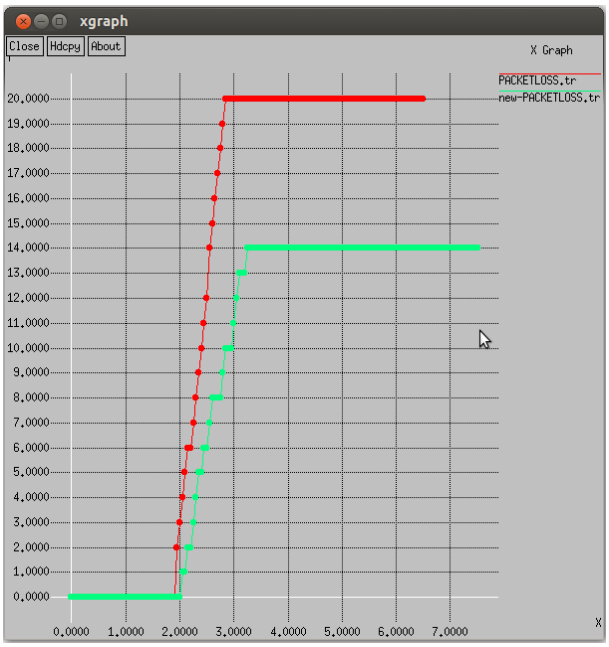

Fig 5: Packet loss comparison

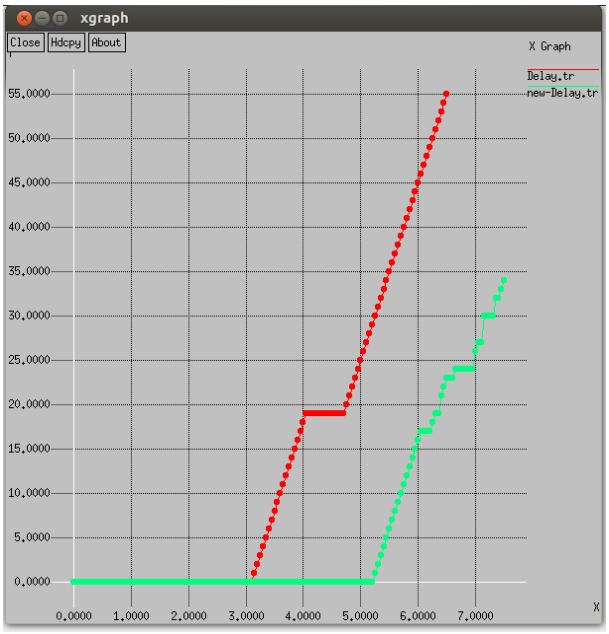

Fig 6: Delay comparison

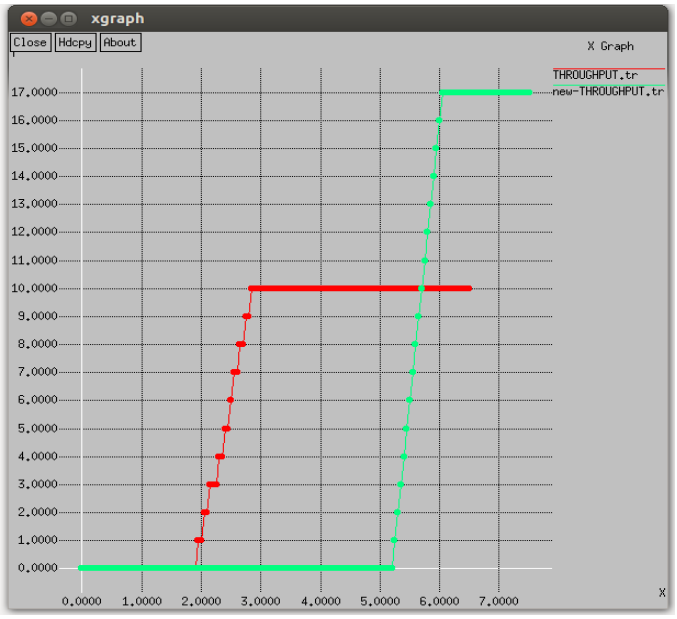

Fig 7: Throughput comparison

VI. CONCLUSION

In this paper, it is concluded that due to the unique properties of the mobile ad hoc network, many security attacks are possible which are prevented by various authentication protocols. In this paper, a novel technique has been proposed which is based on ICMP message to detect and isolate replay attacks in ALARM protocol. The proposed technique has been implemented in NS2 and experimental results are taken in the fixed environment. The results clearly demonstrate that the replay attacks are successfully isolated and detected by using this technique, hence, resulting in increased network throughput and reduced packet loss. In future, we can work to detect and isolate Sybil attacks, which are possible due to ALARM protocol's location assumption.

REFERENCES

[1] Karim El Defrawy, and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", *IEEE transactions on mobile computing*, Vol. 10, No. 9, September 2011.

[2] CaimuTang, and DapengOilver, "An Efficient Mobile Authentication Scheme for Wireless Networks", *IEEE*, 2011.

[3] Tushar Sharma, Mayank Tiwari, Prateek Kumar Sharma, Manish Swaroop, and Pankaj Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet", *International Journal of Engineering Research & Technology (IJERT)*, Vol. 2 Issue 3, March 2013.

[4] Y.V.S. Sai Pragathi, and S.P. Setty, "Hybrid Anonymous Location-Aided Routing Protocol for privacy preserving and authentication in MANET", *Journal of Theoretical and Applied Information Technology*, Vol. 55, No. 2 , 2013.

[5] S. Seys, and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks", *International Journal Wireless and Mobile Computing,* Vol. 3, No.3, pp. 145-155, 2009.
[6] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad-hoc networks", pp. 62-68, 2001.
[7] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, " An overview of Mobile Adhoc Networks: Applications and challenges", SintPietersnieuwstraat 41, Belgium , 2005.
[8] Paul Syverson, "A Taxonomy of Replay Attacks", 1994.
[9] Tarunpreet Bhatia, and A.K.Verma "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms", *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. 3, Issue 6, June 2013.
[10] Cédric Adjih, Emmanuel Baccelli, and Philippe Jacquet, "Link State Routing in Wireless Ad-Hoc Networks", *Proc. IEEE Conf. Military Comm.,* Vol. 2, 2003.
[11] Yixin Jiang, Chuang Lin, Minghui Shi, and Xuemin Shen, "Multiple Key Sharing and Distribution Scheme With (n,t) Threshold for NEMO Group Communications", *IEEE,* 2006.
[12] Steven M. Bellovin and Michael Merritt, "Limitations of the Kerberos authentication system", *USENIX Conference Proceedings*, pages 253-267, Dallas, TX, Winter 1991.
[13] Sushma Yalamanchili, and K.V.Sambasiva Rao, "Two-stage authentication for wireless networks using dual signature and symmetric key protocol", *International Journal of Computer Science and Communication*, Vol. 2, No. 2, pp. 419-422, July-December 2011.
[14] Rohini Sharma, and Minakshi Sharma, Multiple Cooperative black hole attack detection in Mobile Ad-hoc networks", *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC),* ISSN No. 2278-9448, Vol. 4, Issue 2, pp. 83-92, Apr 2014.
[15] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada, "On Alarm Protocol in Wireless Sensor Networks", 2010.
[16] Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer, 2006.
[17] Y.C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", *Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications*, pp. 3-13, 2002.
[18] Sunil Taneja, Dr. Ashwani Kush, and Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", *IJCST*, Vol. 2, Issue No.1, March 2011.
[19] B. Forouzan, "ICMP", in *Data Communication and Networking*, Fourth Ed., McGraw-Hill, 2006, ch.21, pp. 621-637.
[20] "Mobile Ad hoc Networking (MANET) with AODV", *Nova Engineering Inc*., USA, Rep-1.0, 2003.
[21] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", 2005.
[22] Rajinder Kaur Khera, and Rohit Sethi, "Enhancement in ALARM Protocol to prevent Replay Attack in MANET", *International Journal of Engineering Research & Technology*, Vol. 2, Issue 5, ISSN: 2278-0181, May 2013.
[23] Seung Yi, and Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", *10th IEEE International Conference on Network Protocols (ICNP'02),* No.1092-1648, 2002.
[24] Humayun Bakht, " Survey of Routing Protocols for Mobile Ad-hoc Network" , *International Journal of Information and Communication Technology Research,* Volume 1, No. 6, ISSN-2223-4985, Oct 2011.
[25] Padmini Misra (2000). "Routing Protocols for Ad Hoc Mobile Wireless Networks", [online], Available: http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/
[26] "Internet Control Message Protocol", (2014), [Online]. Available:
[27] http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
[28] "Monitor Mode" (2014), [Online]. Available: http://en.wikipedia.org/wiki/Monitor_mode
[29] W. Stallings, "Data Communication", in *Data and Computer Communication,* 7th Ed., Prentice Hall, 2003, ch. 1, pp. 10-14.
[30] Tien-Ho Chen, and Wei-Kuan Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks", *ETRI Journal*, Vol. 32, No. 5, October 2010.
[31] Y.C. Hu , D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", *Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications,* pp. 3-13, 2002.
[32] J. Kim and G. Tsudik, "SRDP: Securing Route Discovery in DSR," *Proc. Mobiquitous*, 2005.

