A DEFENSIVE MECHANISM CROSS LAYER ARCHITECTURE FOR MANETS TO IDENTIFY AND CORRECT MISBEHAVIOUR IN ROUTING

G. S. Mamatha

Department of Information Science and Engineering, R. V. College of Engineering, Bangalore, India
mamatha.niranjan@gmail.com

Abstract

The emerging mobile technology has brought revolutionized changes in the computer era. One such technology of networking is Mobile Ad hoc Networks (MANETS), where the mobility and infrastructure less of the nodes takes predominant roles. These features make MANETS more vulnerable to attacks. As the research continues several aspects can be explored in this area. At the very first it can be the problem of how to make the cross layer detection of attacks more efficient and work well. Since every layer in the network deals with different type of attacks, a possible viewpoint to those attack scenarios can be presented so that it can be extended in the later part. It becomes necessary to figure out the security solution architecture if there are different detection results generated by different layers. Secondly, there should be a measure of the network metrics to show increased performance. The paper presents such a defensive mechanism cross layered architecture which strives to identify and correct misbehaviour in MANETS especially with respect to routing layer. The evaluation of the proposed solution is also given with results obtained to show the performance of the network.

KEYWORDS

Cross Layer Detection, MANETS, Security, Attacks, TODV

1. INTRODUCTION

The vulnerability of MANETS lies in its salient features such as broadcast radio channels, lack of central authority, lack of association, limited resources availability etc;. The paper concentrates on coming out with secured defensive mechanism cross layer architecture for MANETS. Designed with a new routing mechanism it can be called a protocol less approach, encryption technique and an acknowledgement approach, the architecture ensures that it safe guards the data packet forwarding to maximum extent. Thereby the proposed mechanism covers the security aspects of three layers as presentation layer, transport layer and network layer. In any of the systems, one cannot expect the three components I.e. providing security, detection and correction and recovery for transmission to be present; consequently, dealing with an infrastructure-less MANETS will be a dilemma, yet the approach presented for each of these components is independent in nature, providing unusual solutions for each one of them but concentrating mainly on the detection and correction category using a newly proposed routing mechanism TODV (Time On Demand Distance Vector). The contributions of this paper are fourfold. First, we define a ***MANETS Security Solution Architecture (SSA)***. The proposed security solution architecture is a comprehension model which strives to provide end-to-end security for not only MANETS, but all kind of wireless networks for predicting, detecting and correcting security vulnerabilities that may be faced during data communications. As a main step to SSA, it identifies the required security requirements based on their objectives and also

DOI : 10.5121/ijnsa.2012.4111

describes how they can be applied to MANETS and also taking in to account the types of network layer attacks they may face in networking sessions. Second, realization of different levels applied to SSA and illustration of the security requirements confined to these levels such as *authentication*, *availability*, *data confidentiality and data integrity*. The proposed routing mechanism TODV is illustrated to show how it selects the route for communication. The novel combination of ACK, PFC (Principle of flow conservation) and TODV is applied to one of the levels to ensure high security against threats. Through the real time simulation we can test the performance of the proposed security mechanism and demonstrate its effectiveness. Our architecture strives to provide a new novel security protocol less routing that provides a high level of secure, available, scalable, flexible and efficient management services for MANETS. The third contribution is realizing the security attacks which lies within the detection component, which is represented by intentionally launching an attack and identification of the type of attack. This mechanism will be useful to detect malicious nodes which try to bring the system down. The approach presented in the paper as a part of detection level and correction levels can also be applied by varying the network density to study the impact of performance which is validated using an attacks case. The fourth is the cross layer functionalities used for detection of network layer attacks.

In this paper the proposed SSA for MANETS provides a comprehensive, end-to-end security solution that could be applied to every wireless network that satisfies the MANETS requirements. This solution allows us to predict, detect and correct security vulnerabilities that any system might face and so only called defensive mechanism architecture. The paper is organized as follows: in section 2 related works with respect to cross layer anomaly detection is discussed. In section 3, the MANETS Security cross layer architecture is proposed. The security solution architecture identifies the newly proposed routing mechanism TODV, security requirements, and security levels and proposes an end-to-end security solution for MANETS. Section 4 shows the security attacks the system might face. Section 5 explains the evaluation of SSA. Section 6 presents the results obtained as we evaluate the SSA. In Section 7, the conclusions will be drawn.

2. RELATED WORK

The proposed defensive cross layer mechanism exhibits a very good solution for identifying and correcting misbehaviour in MANETS. Many approaches are suggested to improve the performance of MANETS against attacks by using cross layer designs. In order to ensure the authenticity and integrity of routing several key generation and management techniques have been used . Mainly the authentication based approaches ensure the integrity and authenticity of routing messages such as [1], [2]. Some of the cryptographic techniques used to secure MANETS in the later stage proved to be problematic and expensive because of their computational complexity. Even some of the approaches used for intrusion detection have not up to the expectations as they fail to give proper results and explanations like in [3]. Anomaly detection techniques are discussed by A Mishra [4] but no detailed solution or implementation is discussed. Another paper [5] by Haung gives correlations among the nodes and routing anomalies. Loo [6] uses an clustering approach for network layer attacks in sensor networks, and is working only for medium size networks and not scalable. In paper [7], a geometric framework for unsupervised anomaly detection is used but works only for one kind of data like text [8]. Herewith we are presenting a new defensive cross layer architecture which protects the data along with a protocol less routing technique and works for all different kinds of data like text, image and graphics.

3. SECURITY SOLUTION ARCHITECTURE (S S A)

It becomes very crucial to consider security along with the design of the system, rather it should be considered as an inseparable aspect in the development of the system as it is learnt from the

history of security attacks [9]. This criterion makes the proposed security cross layer architecture design to address the global security challenges of consumers, users, services and other applications, thereby covering the security requirements for three of the major layers in the network. The encryption of the data takes place in presentation layer ensuring that the data transmission is safer in lower layers, further the proposed architecture uses a protocol less routing technique in the network layer to choose the optimal path which reduces the network overhead as it stores only needed routes and again an acknowledgement service of transport layer is applied to account the successful transmissions.

3.1. Security Requirements

A set of security requirements are used to address and measure a particular aspect of network security, which is governed by a specific set of security policies. In the mentioned security architecture 4 major requirements that protect the MANETS against all major network layer security threats have been addresses; these requirements are:

- *Authentication* is one of the security measures which reveal the correct identity to both the communicating parties. The verification of communicating parties' identity is a must to confirm that the right parties are on the line.
- *Availability measure ensures* that entities, services and resources are available against all kinds of attack.
- *Data Confidentiality* measure means that the messages or packets are secured from any unauthorized access. Using this kind of security measure it can be easily understood that the information cannot reach the unauthenticated nodes. This can be achieved by applying any of the available encryption techniques.
- *Data Integrity* measure ensures that the messages are unaltered during any communication. The data in communication is protected against unauthorized modification, deletion, creation and replication.

The security requirements illustration is highly important to show how they can protect our system against all major security threats, to provide a comprehensive, end-to-end security solution for MANETS.

3.2. Network Security Levels

The proposed MANETS solution is logically separated into 4 architectural components called network security levels. The OSI [10] model which is useful in designing network protocols is a good example to follow in designing security protocols. This type of component architecture can provide advantages such as modularity, simplicity, flexibility and standardization of protocols. Figure 1 depicts the four network security architecture levels for MANETS, which are built upon one another to provide a network-based solution. The functionality of each level is explained below.

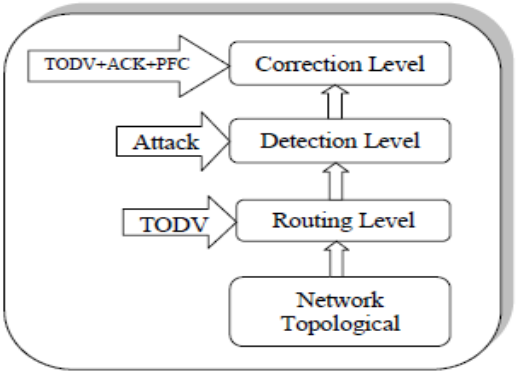


Fig. 1. Network Security Levels

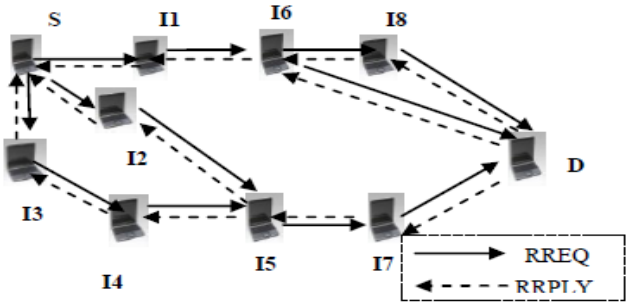
Network Topological Level: The level represents a fundamental building block of the network, consisting of the basic connections between nodes. The first node selected for communication becomes the source node and all the nodes in the middle till they reach the destined node will be the intermediate nodes. The node mentioned in the packet header of the source node will be the destination node. All these nodes identity will be shown clearly using the topological information with indicating the nodes with different colors. This level outlines our assumptions regarding the properties of the physical and network layers. Throughout this paper, an assumption is made for bidirectional communication. Such symmetry of links is needed for the transmission of the designed ACK packets, which conforms to transport layer. Our scheme works with on demand protocol less routing mechanism, such as the proposed TODV (Time on Demand Distance Vector routing) [11] [12]. Further assumption is made that there will be no collusion among misbehaving nodes. A panel will be selected in the terrain area of the simulation environment which displays the number of nodes across the area randomly with incorporated mobility feature. This particular level incorporates the *availability* security requirement feature, with network available for communication as and when needed.

Routing Level: The routing level consists of basic transports and connectivity security mechanisms applied to routing protocols as well as the individual nodes. Every node in the ad hoc network acts as host and router and henceforth the considered solution is not different from that perspective. Moreover, nodes must exchange information about their neighbors to construct the network topology in order to apply any of the ad hoc routing protocols (Proactive, Reactive and Hybrid) [13]. All the nodes in the network must participate in the routing activity, which makes the network connected. Routing security level involves two aspects: secure routing and secure data forwarding. In secure routing all the nodes should cooperate in order to share correct routing information, thus keeping the network connected efficiently, whereas in secure data forwarding, data packets must be protected from message tampering, eavesdropping, and replicating by any of the unauthenticated party [14]. This marks as a route discovery phase in the architecture level and is carried in accordance with the data forwarding protocol employed. In this proposed architecture, a newly proposed on demand protocol less routing mechanism TODV (Time On Demand Distance vector) loosely based on AODV is suitable because, TODV is a hop-by-hop routing process, which introduces a more dynamic strategy to discover and repair route on the par to other on-demand protocols. Instead of destination sequence numbers as in AODV, here we have time concept applied based on first come first served basis. The employed routing process TODV strives to maintain only needed routes in order to reduce the network overheads and to control the network traffic. This situation is applicable for network scenarios where mobility and density are having a moderate picture [15]. The explanation of TODV routing is as follows:

The main concepts of AODV protocol like RREQ (Route Request) and RRPLY (Route Reply) routing packets have been considered in this paper. In the proposed route discovery process the RREQ carries Source Identifier (SID), Destination Identifier (DID) and a Route Node Collection packet (RNC). The SID denotes the source address, DID denotes the destination address and the RNC packet contains the intermediate node IDs address through number of hops as shown in figure 2. That is the RNC packet gives the route definition with total number of hops defined to every node it has visited. As mentioned earlier the limit for RREQ is 3 set for any of the source node, which starts flooding RREQs through the network. Once the RREQ reaches every node, it checks the DID with itself and if not matched forwards further to the next neighboring nodes. In this modified protocol version the RNC packet has different route node collection information. Every node maintains route information about the neighboring nodes. Every RREQ to a destination node generates a Route Reply (RRPLY) packet. The RRPLY packet contains a SID, DID and a RNC packet. Here the notations change, as the SID denotes the destination node address, DID refer to the source node address and RNC again gives the route information it has collected through the RREQ process. In RRPLY DID takes data from RNC to which node it has to pass the RRPLY until it reaches source node. The RRPLY will

come from different routes to source node. The first come first served basis is applied here instead of considering the destination sequence number concept. The RRPLY which arrives first, means which takes minimum time to reach source node will be the shortest path in that instance of time; this is because the MANET topology is dynamic in nature. To count the time of every RRPLY that arrives back to source node a clock will be set at the chosen source node. As the next step the path chosen will be considered for data communication between source and destination nodes. Parallely the other alternative routes possible will also be maintained in database, in case if first route is proved to be malicious.

Detection Level: This level outlines the detection procedure proposed according to the architecture and levels presented in figure 1and 2 respectively. At first the route discovery will be done and then the packets in the information will be get divided in to 48 bytes each. With the fields like SID, DID, the original message with decryption algorithm details, which is protected and can be extracted only when the DID matches with node having the same DID and encrypted message the data frame is constructed. The encrypted information can be accessed by all the intermediate nodes that appear in the route selected for communication. A simple encryption method with replacement of characters by the next alphabet is employed in the proposed detection level of the architecture, which conforms to presentation layer security requirement. In order to count the number of sent packets and number of missed/received packets two counters have been kept at sender node (Cpkt and Cmiss). If the adversary tries to tamper the message, even a small change will be reflected when comparing with the original message at the destination node. Once the data reaches destination, the addresses are matched and only then the fields in the data frame are extracted by the receiver node and decrypts it with the information available in one of the fields in the extracted header. Then the decrypted message is matched with the original message sent. In case both the messages matches, then destination node prepares an acknowledgement frame with an "ACK" field and sends back to the sender through the same intermediate nodes. Such nodes can be called genuine nodes. Else the data frame with "CONFIDENTIALITY LOST" field is sent back to the sender node and indicates the tampering of message. Such a link reveals that an intermediate node is acting as an adversary. Then the RTT (round trip time) is calculated as the difference between the end and starting time of data forwarding for each of the messages sent in milliseconds [15]. The current level mentions the three of the security requirements, authentication, and data integrity and data confidentiality. If there is a violation in these requirements as the next step a corrective measure is taken to identify the type of attacks and choose an alternative link in the correction level.



S-Source, D-Destination, I1 to I8-Intermediate nodes
Consider RREQ1 from S to I1:
RREQ1: (SID, DID, RNC= ({S → I1 → I6 → D}, 3 Hops))
RREQ1: (SID, DID, RNC= ({S → I1 → I6 → I8 → D}, 4Hops))
RRPLY1: (DID, SID), {D → I6 → I1 → S})
RRPLY1: (DID, SID), {D → I8 → I6 → I1 → S}

Figure. 2. A Scenario of MANET showing the contents of RNC Packet

Correction Level: A time limit for RTT is set to 20ms or more according to the application. If the sender node gets the acknowledgement back exceeding the time limit, it indicates of packet loss. On the other end of the sender node parallely a counter to keep track of lost packets (Cmiss) is kept and incremented if an acknowledgement reaches exceeding time limit. The procedure is repeated for all the data packets sent. Later based on the principle of flow conservation a ratio of Cmiss/Cpkt will be calculated [16]. The threshold value for evaluating the ratio is set to 20% (0.2) called limit of tolerance ratio. The route chosen is evaluated for the ratio after completing the transmission. If the ratio exceeds the limit set then it is said to be misbehaving link. The further communication happens by choosing the alternative link available in the data base within few milliseconds. If sender finds the "CONFIDENTIALITY LOST" field in the acknowledgement frame then it comes to know about the malicious node from the routing table information which has tampered the message, maintained by the sender node. Such links which exceeds limit of tolerance ratio and has the above information in their acknowledgement is discarded for further session [15].

4. NETWORK SECURITY ATTACKS

The security plays a vital role in ad hoc wireless networks, especially in military applications. The lack of any central association makes MANETS more vulnerable to attacks than wired networks. Consequently, the network security attacks in MANETS are generally divided into two broad categories, namely, Passive and Active attacks. A passive attack refers to the attempts that are made by malicious nodes to perceive the nature of activities and to obtain information transacted in the network without disrupting the operation. For example, eavesdropping, active interference, leakage of secret information, data tempering, impersonation, message replay, message distortion and denial of service. Detection of passive attacks is complicated, since the network operation is not affected. One good solution to overcome such problems is through encryption methods, encrypting the data being transmitted, thereby making it hard for eavesdroppers to gain any active information from the data being transmitted. An active attack refers to the attacks that attempt to alter, inject, delete or destroy the data being exchanged in the network. These attacks can be prevented by using regular security mechanisms such as encryption techniques and firewalls. Internal attacks are more serious and difficult to detect than external ones. The brief descriptions of some of the main active attacks known in most networks [17, 18, 19, 20, 21 and 22] [23] are described in the paper [24]. The attacks that occur in the network layer, when several types of attacks are mounted on the routing protocols which are aimed at disrupting the operation of the network. Some of the major routing layer attacks are described briefly in the paper [24].

5. EVALUATION OF SSA

The section mainly discusses the methodology used to evaluate the performance of the proposed defensive cross layer security mechanism as SSA. It explains the different evaluation metrics and the simulation environment used to test them, as shown in Figure 4. The behaviour of the SSA in real time simulation network environments needs to be tested, the overhead caused by the proposed security protocol less routing strategy is to be measured and the time needed to perform successful simulation without attacks is to be calculated. Therefore, a suitable network simulator must be chosen to provide the communication performance of the proposed security mechanism. This section will justify the application of the real time simulator used and developed at the par to standard simulators to simulate the security mechanism, as well as showing how the simulation environment is set, what are the simulation metrics and the network metrics used to measure performances [23].

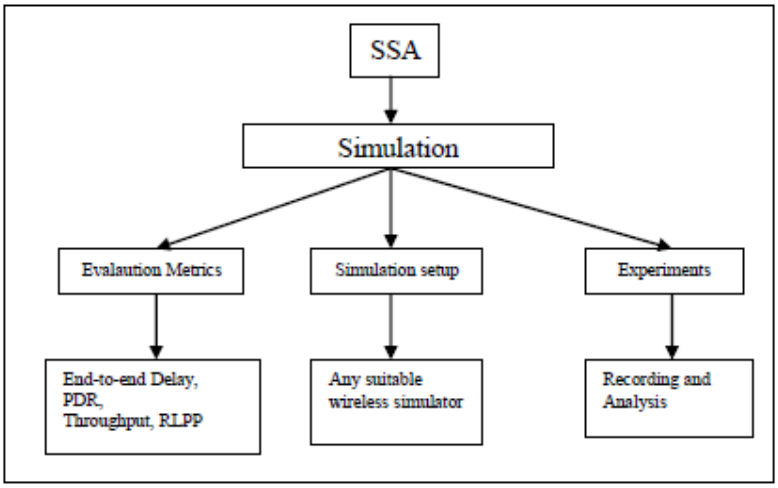


Figure. 3. Evaluation of SSA

6. RESULTS

As mentioned in the evaluation of SSA, the experimental and simulation methods are carried out to measure the performance thereby detecting and correcting the misbehavior in network layer and shown in [15].

A simulation environment at the par to standard simulators is implemented to show the performance of MANETS with 30 mobile nodes assuming in the transmission range of 250 mts and with a mobility speed of 10 mts/sec. The evaluation is done by varying the packet size, attacks and keeping the source constant with different destinations. The evaluation is carried in three situations as ideal, with attack and with correction. The values of the network parameters considered for evaluation are throughput, delay and overhead. The values for all the network metrics in all the three situations i;e ideal (without attack or normal) situation, with attack situation (WA) and with correction (WC) situation is measured and compared.

The following figure 4,5and 6 shows the network metrics performances with other data as considered below:

Number of simulation runs conducted = 10

Packet size considered = 16 bytes, 32 bytes and 48 bytes

Attack type = Message Tampering

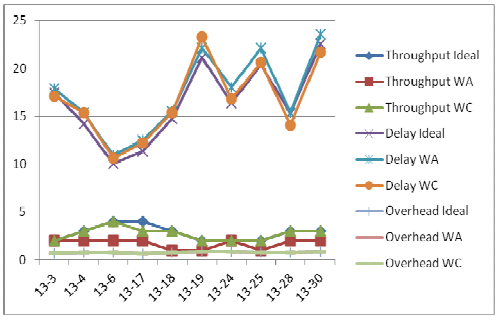


Figure 4. Performance measure of message tampering attack for 16 bytes of data

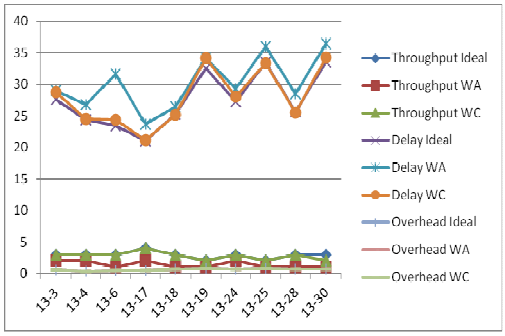


Figure 5. Performance measure of message tampering attack for 32 bytes of data

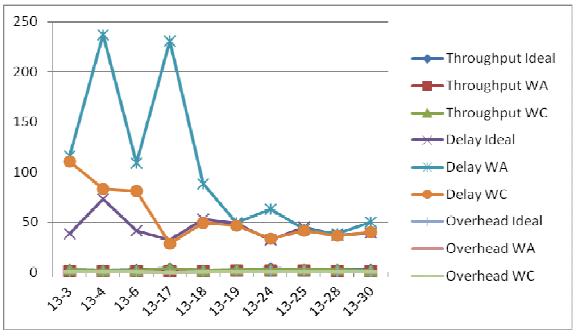


Figure 6. Performance measure of message tampering attack for 48 bytes of data

The following figure 7,8 and 9 shows the network metrics performances with other data as considered below:
Number of simulation runs conducted = 10
Packet size considered = 16 bytes, 32 bytes and 48 bytes
Attack type = Gray hole attack

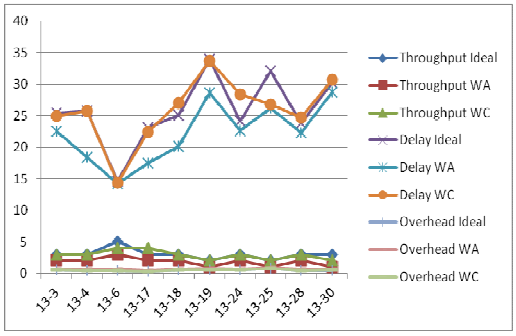


Figure 7. Performance measure of Gray hole attack for 16 bytes of data

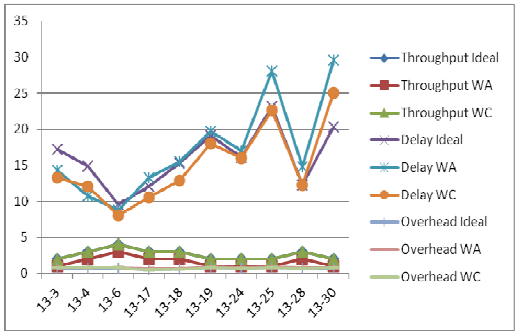


Figure 8. Performance measure of Gray hole attack for 32 bytes of data

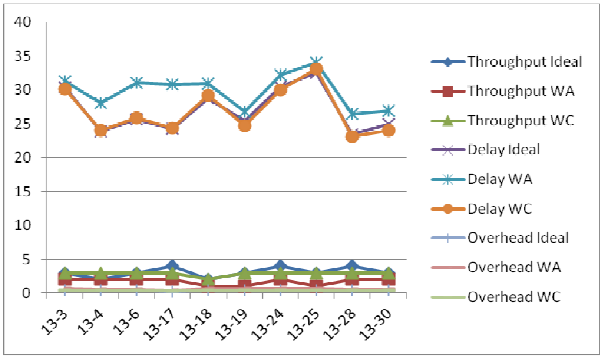


Figure 9 Performance measure of Gray hole attack for 48 bytes of data

The performance measure with varying destinations, keeping source constant and varying the packet size, attack types is clearly shown in all the figures as above. It is very clear that when compared to ideal and corrective situation the performance degrades in attack situation. This is how the proposed cross layer defensive architecture provides an extended security to MANETS with considerable increase in the performance when compared to the existing approaches

7. CONCLUSION

Designing a clear line of defense in MANETS is a very tough task. Herewith we have come with a possible security solution in the form of cross layer architecture known as SSA. This SSA fulfils some of the main security requirements as we mentioned, further it can be extended to more also. The security and encryption mechanisms can also be varied according to the simulation environments and applications. We are also ensuring that the routing technique mentioned namely TODV also works at the par to satisfy the MANET requirements. As the results shown with simulation experiments conducted states that the proposed approach guarantees the security objectives for MANETS and shows considerable enhancement in performance.

REFERENCES

[1] K. Sanzgiri, B. Dahill, B.N. Levine, E.B. Royer, and C. Shields, "A Secure Routing Protocol for Ad-hoc Networks," *in the Proceedings of International Conference on Network Protocols (ICNP)*, 2002.

[2] Yih-Chun Hu, Adrian Perrig, and David Johnson. Ariadne: "A Secure On- Demand Routing Protocol for Ad Hoc Networks," *in the Proceedings of MobiCom*, 2002.

[3] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM J. Wireless Networks*, pp. 545-556, 2003.

[4] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad-Hoc Networks," *in IEEE Wireless Communications*, pp.48- 60, February 2004.

[5] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," *in the Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS) Providence*, pp. 478-487, 2003.

[6] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in *International Journal of Distributed Sensor Networks*, pp. 313-332, october-December 2006.

[7] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, S. Stolfo, "A geometric framework for unsupervised anomaly detection: detecting intrusions in unlabeled data," *in Applications of Data Mining in Computer Security*. Kluwe, 2002.

[8] R. Shrestha et.al. "A Novel Cross layer Intrusion detection system for MANETS", In Proc. of 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 647-654

[9] P. Chandra," Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security", *Elsevier*, 2005.

[10] E. Carrieri, C. A. Rpcchini, A. Fioretti, and A. J. Haylett, "An OSI Compatible Architecture for Integrated Multichannel Metropolitan and Regional Networks", *Integrating Research, Industry and Education in Energy and Communicational Engineering, MELECON '89*, Mediterranean, 11 – 13 April 1989, pp.639 – 643.

[11] S. Capkun, Hubaux, L Buttyan, "Mobility helps security in ad hoc networks", *In proceedings of ACM symposium onmobile ad hoc networking and computing*, June 2003.

[12] S. Capkun, Hubaux, L Buttyan, " Mobility helps peer-to-peer security", *IEEE transactions on mobile computing*, Vol. 5, No. 1, Jan 2006, pp. 43-51.

[13] E. M. Royer, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", *IEEE Personal communication*, April 1999, pp: 46 – 55.

[14] C.E. Perkins, and E.M. Royer, "Ad-hoc on-demand distance vector routing", *In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, WMCSA'99., 25-26 Feb. 1999, pp: 90 – 100.

[15] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS", *International Journal of Computer Theory and Engineering*, Vol. 2, No.5, October, 2010.

[16] Oscar F.G, G. W Ansa, M. Howarth, G. Paylou, " Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad hoc networks", *Journal of Internet Engineering*, Vol. 2, 2008, pp. 1.

[17] J. Al Jaroodi, "Security Issues in wireless mobile ad hoc networks", *Technical Report* TR02-10-07, University of Nebraska-Lincoln, 2002.

[18] C. Siva ram murthy and B.S. Monoj, " Ad oc wireless networks, architecture and Protocols", *Prentice hall communications, Engineering and Emerging technologies series*, Upper saddle river, 2004.

[19] K. Fokine, "Key Management in Ad Hoc Networks", *Master Thesis, Linkping University*, 2002.

[20] A. Mishra, Nadkarni, "Security in wireless ad hoc networks", *Hand Book of Ad Hoc Networks*, CRC Press, FL, USA, 2003, pp. 479-490.

[21] Fei. X, Wenye W, "Understanding Dynamic DoS Attacks in Mobile ad hoc Networks", *In proceedings of MILCOM*, Oct 2006, pp. 1-7.

[22] T. Wen-Guey, "A secure fault-tolerant conference-key agreement protocol Computers", *IEEE Transactions,* Volume 51, Issue 4, April 2002, pp. 373 – 379.

[23] Ali Hilal Al-Bayatti, "Security Management for Mobile Ad Hoc Network of Networks (MANON)", *Thesis* presented in Feb 2009.

[24] G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", *International Journal of Computer Applications* (0975 – 8887), Volume 9, No.9, Nov 2010.