IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

Security Mechanisms for Mitigating Multiple Black hole Attack In Manets

Shikha Sharma[1], Manish Mahajan [2]

[1]Research Scholar, CGC College of Engineering,Landran Road, Mohali, India.

[2] HOD, COE College of Engineering,Landran Road, Mohali, India

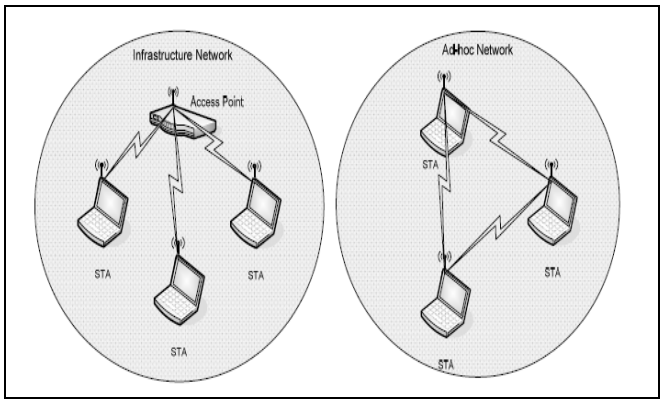
Abstract

Wireless adhoc networks are decentralized, self-organizing networks capable of forming a communication network without relying on any fixed infrastructure. This type of wireless network requires rapid and automatic establishment of services in the absence of a fixed. Mobile Ad hoc Networks (MANETs) do not have a centralized piece of machinery, which could lead to a single point of failure and the consequent absence of authorization facilities, thus, make the network that much more vulnerable. Security have recently become very important and actively researched topics because of a growing demand to support live streaming audio and video in civilian as well as military applications. Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation. In this paper, the behavior of multiple black hole attacks and the performance impact of this attack on AODV protocol and its counter measures using IDS AODV and Watchdog AODV scheme is studied. The NS2 network simulator is used for evaluation.

Keywords: *AODV, IDS, MANETs .*

1. Introduction

Wireless technologies are being widely used today across the globe to support the communications needs of very large numbers of end users. There are several reasons for the current popularity of wireless technologies such as cost, communication area etc. Wireless networks can be classified in two types: - infra-structured network and infrastructure less (ad hoc) networks. A Mobile Ad Hoc Network (MANET) is an autonomous system of mobile nodes with routing capabilities connected by wireless links, the union of which forms a communication network [4]. The versatility of MANETs makes them ideal candidates for a wide-range array of applications. Although implementing a MANET is a very challenging task, several applications exist that try to surmount the aforementioned difficulties. The most widely discussed application scenario for pure general purpose MANET is a battlefield or a disaster-recovery network, however these kinds of networks have not achieved the envisaged impact in terms of real world implementation and industrial development [1]. Mobile ad-hoc networks offer unique versatility for certain environments and certain applications. Since no fixed infrastructure, including base stations, is prerequisite, they can be created and used any time, anywhere. Indeed, since all nodes are allowed to be mobile, the composition of such networks is necessarily time varying. Addition and deletion of nodes occur only by interactions with other nodes; no other agency is involved. Such perceived advantages elicited immediate interest in the early days among military, and rescue agencies in the use of such networks, especially under disorganized or hostile environments, including isolated scenes of natural disaster and armed conflict.



(a) Infrastructure Network (b) Adhoc Network

Figure 1 Wireless Networks

Wireless ad hoc networks promise an unprecedented fine-grained interface between the virtual and physical worlds. They are one of the most rapidly developing new information technologies, with applications in a wide range of fields including industrial process control, security and surveillance, environmental sensing, and structural health monitoring. Because of their pervasive and sometimes critical surveillance operation, the data collected by ad hoc networks must be kept private, and networks must also be protected against malicious attacks aimed at disrupting or disabling their functionality.

A. Security Issues and Challenges

The special properties of ad hoc networks enable all the neat features such networks have to offer, but at the same time, those properties make implementing security

ISSN 2348 – 7968

protocols a very challenging task. One of the fundamental vulnerabilities of MANETs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well-defined place or infrastructure where we may deploy a single security solution. There are four main security problems that need to be dealt with in ad hoc networks:

(1) the *authentication* of devices that wish to talk to each other;

(2) the *secure key establishment* of a session key among authenticated devices;

(3) the *secure routing* in multi-hop networks; and

(4) the *secure storage of (key)data* in the devices.

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation.

- *Confidentiality* is to keep the information sent unreadable to unauthorized users or nodes. MANETS uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas.
- *Authentication* is to be able to identify a node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANETS, and it is much more difficult to authenticate an entity.
- *Integrity* is to be able to keep the message sent from being illegally altered or destroyed in the transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack.
- *Non-repudiation* is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.
- *Availability* is to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents.
- *Access control* is to prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

The network infrastructure of a MANETs is made up of small, cheap nodes spread over a possibly hostile area. Unlike other types of networks, it is often impossible to prevent the ad hoc nodes from being physically accessed by attackers. This is also referred to as node capture. It is reasonable to assume that an attacker can achieve full control over a captured node that is he can read its memory or influence the operation of the node software. Special secure memory devices would be needed to prevent the attacker from reading the memory; however, these will only rarely be present in cheap ad hoc nodes. The constraints regarding memory and computational capabilities are a serious obstacle for implementing cryptographic algorithms. Especially asymmetric key cryptography is considered too heavyweight for small processors, let alone the key management involved. When in-network processing is to be performed, intermediate nodes need to access and modify the information contained in packets; hence, a larger number of parties is involved in end-to-end information transfers.

B. Security Attacks

A variety of attacks are possible in MANETs. Some attacks apply to general network, some apply to wireless network and some are specific to MANETSs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in MANETS and all other networks can be roughly classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

Passive vs. active attacks: The attacks in MANETS can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANETS.

Internal vs. external attacks: The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are

ISSN 2348 – 7968

more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Table 1 : Attacks on different layers of the Internet model.

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	blackhole, Grayhole, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Attacks on different layers of the Internet model: The attacks can be further classified according to the five layers of the Internet model.

Cryptography vs. non-cryptography related attacks: Some attacks are noncryptography related, and others are cryptographic primitive attacks.

Stealthy vs. non-stealthy attacks: Some security attacks use stealth, whereby the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealthy.

2. Related Work

Smita Karmakar et al.[1], present a brief comparative study of various types of holes and various types of coverage holes. Holes are one of the challenges in deployment of WSNs in a large area. Holes generally considered as a communication gap among sensor nodes. The authors also provides a brief overview two different solutions for hole detection that are proposed by researchers. They are vornoi diagram and triangular oriented diagram. Voronoi diagram approach is used to detect a coverage hole and calculate the size of a coverage hole. A plane area is divided into N cells. Each cell contains one sensor. Two Voronoi cells meet along a voronoi edge. A sensor node is a voronoi neighbour of other sensor node, if they both share a voronoi edge. Voronoi diagram approach has few limitations like shape of each cell is different. So, it is very tough to calculate the exact size of the hole. The limitation of other solution namely triangular oriented structure is that, it is not a proper hole detection solution because, in a large WSNs, it is complex to connect the centre of three adjacent sensors. Here authors also proposed simple and straight-forward algorithm initially find out whether a sensor node is alive or dead. According to this algorithm, when the sensor node is dead, then the geographical area is not covered by that sensor node, so this area will be treated as hole.

Benamar Kadri et al. [2], propose a lightweight implementation of public key infrastructure called cluster based public infrastructure (CBPKI). CBPKI is based on the security and the authenticity of the base station for executing a set of handshakes intended to establish session keys between the base station and sensors over the network used for ensuring data confidentiality and integrity. CBPKI is intended to establish security over the network using three cryptographic methods destined to establish all the security services. CBPKI is based on two handshakes namely Cluster-head to base station handshake and Cluster members handshake. The handshake is executed by each cluster head and the base station is intended to establish a symmetric key be-tween sensors and the base station. propose to launch periodically a proactive key update of the session key; the period of the key update is defined by the administrator according to the length of the used keys as well as the robustness of the encrypting algorithms. The key update is launched by the cluster head using the same hand shake defined above in order to establish a new session key between the base station and the cluster head. After updating the session key of the cluster head, each cluster head encrypts a copy with the old session key for each member of its cluster. The authors also ensures the CBPKI for all security services and checks its robustness against several attacks with low power consumption and network overhead.

Vinh Hoa LA et al. [3], presents a survey of VANETs attacks and their solutions Risks caused by security attacks are one of the major security issues for the VANETs that are constraining the deployment of the vehicular ad hoc networks. The authors presented an upto- date collection of attacks damaging VANETs, sampled the practical scenarios and also discussed the existing solutions to deal with attacks, and characterized each attack to have a thorough look over it. The authors conclude intruder detection as the better mechanism and intend to construct an intrusion detector for VANETs to alert the attacks in the case performing.

Bhimsingh Bohara et al. [4], discuss the effect of gray hole attack and their counter measuring solution over mobile adhoc network. The Grayhole attack is an active kind of attack on adhoc networks where the attacking node first forwards packets and then later on drops the packets resulting in Denial of Service (DoS). The author use Intrusion Detection scheme to report violation of policy

ISSN 2348 – 7968

and the nodes whose packets are dropped again try to establish new paths using Route Requests messages. The Gray hole attack is in a way bit similar to Black hole attack. A black hole attack where drops all the packets, on the other hand the gray hole attacking node drops packet with certain probability. The authors analyzed the effects of gray hole in an AODV network. From simulation results with varying speed and 30 nodes for normal AODV as well as after the inclusion of gray hole in AODV.

D.M. Shila et al [5] offered a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first stage of the algorithm is Counter-Threshold Based and uses the detection threshold and packet counter to discover the attacks. The second stage is Query- Based and uses acknowledgment from the intermediate nodes to confine the attacker. In the first stage, two types of packets, Control packet and Control ACK packet, are used to detect the attacker. Furthermore, they determine the proper value of detection threshold based on the routing Expected Transmission Count metric ETX to improve the performance under different network situation.

Onkar V.Chandure et al. [6], describe the basic idea related with the implementation of AODV protocol and evaluates the impact of gray hole attack on adhoc network. A Gray hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. The authors analyse the impact of gray hole attack on adhoc network for different performance metrices like packet delivery ratio and end to end delay. Simulation of AODV as well as gray hole attack is carried out by using ns-2 simulator.

Chetan S. Dhamande et al. [7], presented a brief study on different for the minimizing the impact of gray hole attack using AODV routing protocol.. Gray hole attack ultimately decrease the performance of the network & also corrupt the data Proposed solution is mainly focus on the miminize the impact of gray hole attack in MANET & also improve the security as well as the performance of the network. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from or destined to certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for Some time duration by dropping packets but may switch to normal behaviour later.

Tarun Varshney et al. [8], investigate more existing mechanisms to prevent blackhole attack and propose a slight modification to AODV, called Watchdog –AODV (WAODV) that detects blackhole attack and also attempt to reduce further rise in normalized routing overhead. This mechanism firstly detects a blackhole node and provide a new route to source node. This mechanism greatly increases reliability of detection and isolation of multiple malicious blackhole nodes during route discovery process and discovers a short and secure route towards destination without introducing additional control packets.

In cryptographic approaches like S-AODV [9] and Adriane [10], the routing packets are encrypted using symmetric or asymmetric algorithm and hence external or inside attacker cannot modify the packets. However the problem with cryptographic approaches is the increased consumption of processing power and flooding attack can also be launched without forging the packets.

In [11] Dahill, et al. proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN end-to-end authentication is achieved by the source by having it verify that the intended destination was reached. In this process, the source trusts the destination to choose the return path. The source begins route instantiation by broadcasting a Route Discovery Packet (RDP) that is digitally signed by the source. Following this, every intermediate node verifies the integrity of the packet received by verifying the signature. The first intermediate node appends its own signature encapsulated over the signed packet that it received from the source. All subsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to the packet.

One primitive solution to vanish the RREP forging is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node [12]. This method avoid intermediate node to reply which avoid in certain case the Black Hole and implements the secure protocol. This increase the routing delay in large networks and a malicious node can take advantage by replying message instead of destination node. So for this one or more routes are used by the intermediate nodes which replay the RREQ messages to confirm the routes from intermediate nodes and destination nodes for sending out the data packets. In case if it does not exist, the reply messages is discarded from intermediate node and alarm messages are sent to the network. This method avoids the Black Hole problem thus preventing the network from malicious node. This will result in great delay especially in large networks and in addition the attacker can fabricate a reply message on behalf of the destination node.

ISSN 2348 – 7968

3. Proposed Methodology

In this paper, we evaluate the performance of AODV routing protocol under multiple black hole attacker nodes and counter measures it using IDS AODV and Watchdog AODV. A number of mechanism were proposed to solve the blackhole problem. It requires a source node that initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination. In this thesis, the behavior of grayhole attack and the performance impact of this attack on AODV protocol and its counter measures using Watchdog AODV scheme is studied. A number of reactive scheme are proposed that can identify the misbehaving node without causing much overhead. The NS2 network simulator is used for evaluation. This simulation process considered a wireless network of nodes which are placed within a 1200m X 300m area. CBR (constant bit rate) traffic is generated among the nodes. The simulation runs for 100 seconds.

Table: Important Simulation Parameters

Parameter	Value
Simulation area	1200m x 300m
Antenna	Omni antenna
No. of nodes	10,15,20,25,30
Simulation time (sec)	100
Traffic	CBR (Constant bit rate)
Routing protocol	AODV,
Security attack	Black Hole attack
Security Mechanism	IDS and Watchdog AODV

Simulations are performed for black hole attack in a multi hop ad hoc network environment. The impact of node's mean pause time on the performance of AODV routing protocol under black hole security attacks and its counter measure using IDS AODV and Watchdog AODV is shown with the help of simulation graphs in terms of throughput, number of packet drops, and packet delivery ratio.

- **Throughput**

The figure 3 shows the effect of black hole attack on the throughput of AODV and its prevention using IDS AODV and Watchdog for different Network size. Fig. 3 shows the measured throughput for AODV routing protocol under blackhole hole attack against prevention mechanism namely watchdog intruder detection scheme is much better than other prevention mechanism.

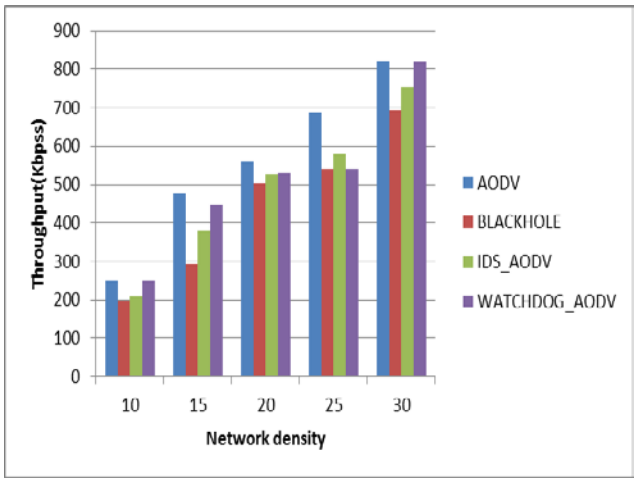


Figure 2: Throughput of of AODV under multiple black hole and its counter measuring techniques IDSAODV and Watchdog AODV.

- **Packet Delivery Fraction**

Figure 4 shows the packet delivery ratio when the network density is varied. The figure depicts that PDR of AODV routing protocol is heavily affected by blackhole attack attack. It has been observed from the simulation scripts that when the AODV protocols are under attack of black hole attack, watchdog-AODV has a more packet delivery ratio, as compared to other prevention mechanism namely IDS AODV.

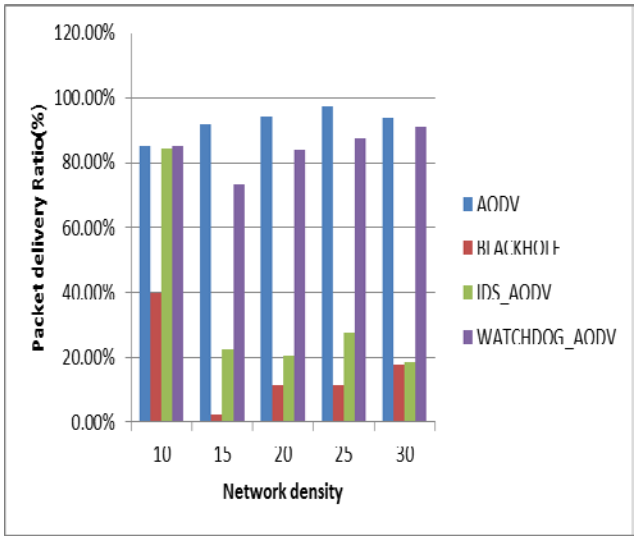


Figure 3: PDF of of AODV under under multiple black hole and its counter measuring techniques IDSAODV and Watchdog AODV.

- **Number of Packet Drops**

ISSN 2348 – 7968

Figure 5 shows the amount of packet drops when network density is varied.The figure depicts that packet drops efficiently reduced in the case of Watchdog AODV routing under blackhole attack as compare to IDS AODV under attack.

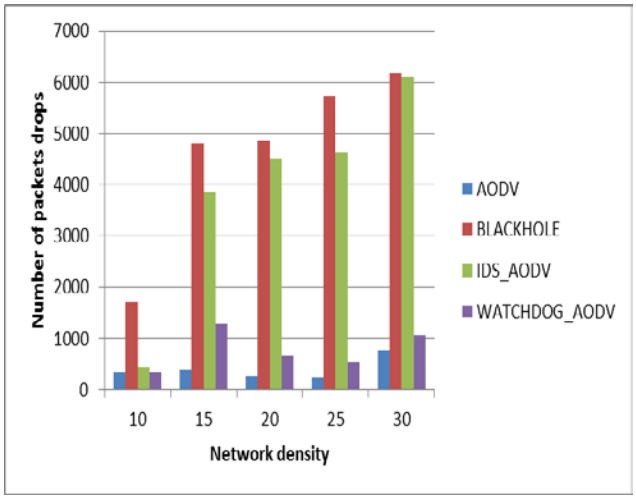


Figure 4: Packet drops of AODV under grayhole and its counter measuring technique Watchdog IDS.

4. Conclusion and Future Work

In this paper, we simulated the black hole attack in the Ad-hoc Networks and investigated its affects. Having simulated the black hole attack, we saw that the performance of AODV is decreased in the ad-hoc network. The security schemes that govern trust among communicating entities are collectively known as trust management. Here trust means the confidence of an entity on another entity based on the expectation that the other entity will perform a particular action important to the one who trusts, irrespective of the ability to monitor or control that other entity. Here we evaluate the effect of multiple black hole attacker nodes on the performance of entire network and compared two possible trust management solution tries to eliminate the black hole effect by monitoring scheme to isolate malicious node from the network. From simulation results, we can conclude that Watchdog IDS trust management solution for preventing black hole attack is much better that other proposed solution. The watchdog does this by listening to all nodes within transmission range promiscuously. If a watchdog detects that a packet is not forwarded within a certain period or is forwarded but altered by its neighbour it deems the neighbour as misbehaving and if any node only accept the node and does not forwarded, watchdog declare that node as a gray hole node and exclude that node from the path of the sending packets.

References

[1] Smita Karmakar and Alak Roy, “Holes Detection in Wireless Sensor Networks: A Survey” Modern Education and Computer Science, MECS, 2014, pp. 24-30.

[2] Benamar Kadri, Djilalli Moussaoui, Mohammed Feham and Abdellah Mhammed, “An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks” Wireless Sensor Network,Scientifi research, June 2012, pp. 155-161.

[3] Vinh Hoa LA and Ana Cavalli “ Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey” International Journal on Ad, Hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[4] Bhimsingh Bohara, Varun Sharma “Analysis and Prevention of effects of gray hole attacks on Routing Protocol in Mobile Ad-hoc Networks” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013.

[5] D.M. Shila, T. Anjali “Defending selective forwarding attacks in WMNs” International Conference on Electro/Information Technology, IEEE, 2008.

[6] Onkar V.Chandure, V.T.Gaikwad “Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol” International Journal of Computer Applications, Volume 41, issue 5 , March 2012.

[7] Chetan S. Dhamande, H. R. Deshmukh “A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network” International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012.

[8] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma “Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network” Fourth International Conference on Communication Systems and Network Technologies, IEEE, Oct. 2014, pp 217-221.

[9] S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

[10] S. Yi and R. Kravets, Composite Key Management for AdHocNetworks.Proc. Of the 1st Annual InternationalConference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous’04), pp. 52-61, 2004.

ISSN 2348 – 7968

[11] Hu, Y., Perrig, A., & Johnson, D. (2002). Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta

[12] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.