ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

# Optimized Efficient Security Mechanism For The Ad-HOC Netwrok

[I]Nidhi, [II]Er. Kapil Arora
[I]M.Tech (Student), [II]A.P
[I,II]Dept. of ECE, RPIIT College, Karnal, Haryana, India

**Abstract**
*A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces. In order to make communication among nodes, the nodes dynamically establish paths among one another. The nature and structure of such networks makes it attractive to various types of attackers. Security is a major concern for protected communication between mobile nodes. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers This paper evaluates the impact of some adversary attack on mobile Ad Hoc Network (MANET) system. We have further make an attempt to introduce some efficient security techniques to provide robust security solution.*

**Keywords**
*MANET, attacks, malicious nodes, active attacks, passive attacks etc.*

## I. Introduction

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. It is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Each node in a MANET is free to move Independently in any direction, and will therefore change its links to other devices frequently; each must forward traffic unrelated to its own use, and therefore be a router. The MANET network enables servers and clients to communicate in a non-fixed topology area and it's used in a variety of applications and fast growing networks.

With the increasing number of mobile devices, providing the computing power and connectivity to run applications like multiplayer games or collaborative work tools, MANETs are getting more and more important as they meet the requirements of today's users to connect and interact spontaneously.

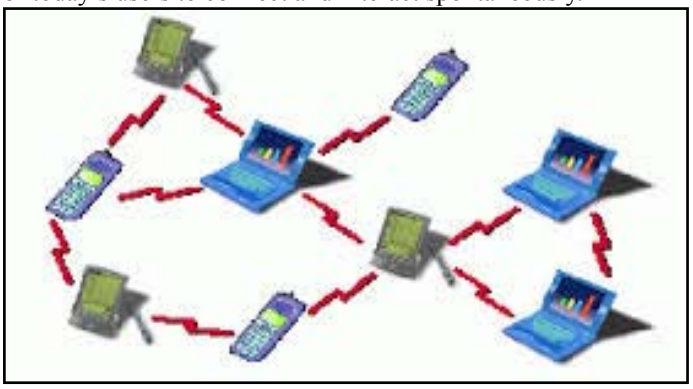

Fig.1 : Mobile ad-hoc network

### A. Characteristics

- The nodes can join or leave the network anytime, making the network topology dynamic in nature
- Mobile nodes are characterized with less memory, power and light weight features
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

## II. Security in Manet

Mobile Ad-hoc Network (MANET) is different from the traditional wired networks due to its mobility, infrastructure less topology and the absence of central authority in the network. Any system that has to be protected might have weaknesses or vulnerabilities, some or all of which may be targeted by an attacker. Hence, one approach to designing security mechanisms for systems is to look at the threats that the system faces and the attacks possible given the vulnerabilities. The design security mechanisms should then ensure that the system is secure in the light of these threats, attacks, and vulnerabilities.

## III. Vulnerabilities

The vulnerabilities of MANETs are summarized below

- **Wireless links:** First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks.
- **Dynamic topology:** MANET nodes can leave and join the network, and move independently. As a result, the network topology can change frequently. It is difficult to differentiate normal behavior of the network from anomaly/malicious behavior in this dynamic environment.
- **Co-operativeness:** Routing algorithms for MANETs usually assume that nodes are cooperative and non malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications.
- **Lack of clear line of defense:** MANETs do not have a clear line of defense; attacks can come from all directions. The boundary that separates the inside network from the outside world is not very clear on MANETs.
- **Limited resources:** Resource constraints are a further vulnerability. There can be variety of devices on MANETs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of

new attacks.

## IV. Attacks

MANETs often experience unusual security attacks because of their following features such as dynamically changing topology, lack of central monitoring, mutual algorithms and absence of a centralized certification authority etc. Generally mobile ad hoc networks are affected by two kinds of attacks which are classified as passive and active. Passive attacks do not affect the functionality of network, but may attempt to find out vital information by listening to traffic. It is difficult to identify such attacks as under these attacks the network operates normally. These attacks basically obtain critical routing information through sniffing. Such attacks are usually complex to identify and protection against such attacks is also difficult. Moreover, it is sometimes not even possible to trace the exact location of the attacker node. Generally, such type of attacks is prevented with the help of encryption.

**Table 1.** Some Attacks on the Protocol Stack

| LAYERS | ATTACKS |
|---|---|
| Application layer | Data corruption, viruses and worms |
| Transport layer | TCP/UDP SYN flood |
| Network layer | Hello flood, black hole, worm hole |
| Data link layer | Monitoring, traffic analysis |
| Physical layer | Eavesdropping, active interference |

## V. Some More Harmful Attacks

### A. Black Hole Attack

Black hole attack is also an important and suspicious attack in mobile ad hoc networks. It sends fake or false routing information to the source node that it has fresh routing path from source to destination. In on-demand routing protocol, if a source node S starts to send route request(RREQ) packets to initiate the transmission. At that time, S sends route request packets to its neighbors. They are forwarding the packets to their neighbors. In this way the route request packets are sent up to the destination. In black hole attack, the attacker captures the route request packets and sends route reply(RREP) packets back to the source node S that it has the fresh route from S to destination D. Source node S discards the other route reply packets that are coming from other route. After getting the route reply from attacker node, S decides to send the further data along that path. But the data is transmitted only to the attacker node. And attacker node will decide whether the data may

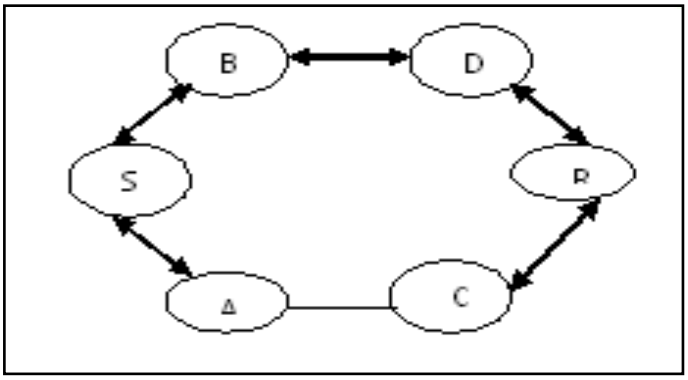


Fig. Black hole Attack

### B. Worm Hole Attack

Wormhole attack is a silent and severe type of attack since it simply copies the packet at one location and replays them at different location or within the same network. So, in wormhole attack, there are two neighbor malicious nodes. They copy the packet at one location and replay the same packets without any changes in the content at different location or within the same network.

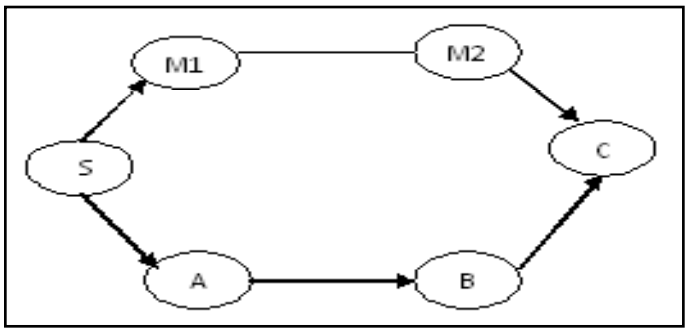


Fig. Wormhole Attack

## VI. Simulation Results

We have proposed the method to improve the system's efficiency using different routing protocols (AODV, DSDV etc). We have also proposed a method to countermeasure these attacks using elliptical security keys.

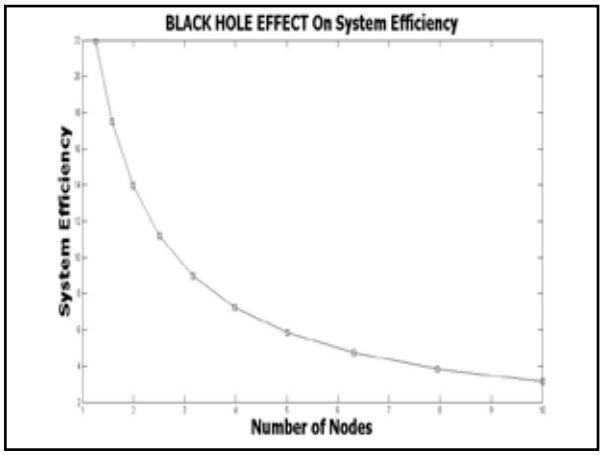


Fig. 6.1: Black hole effects on system efficiency

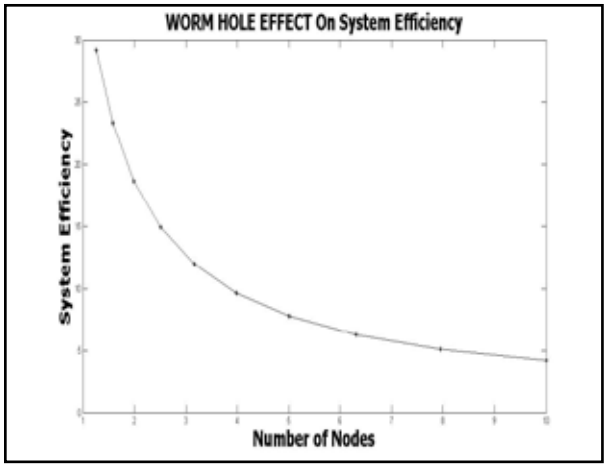


Fig. 6.2: worm hole effects on system efficiency

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

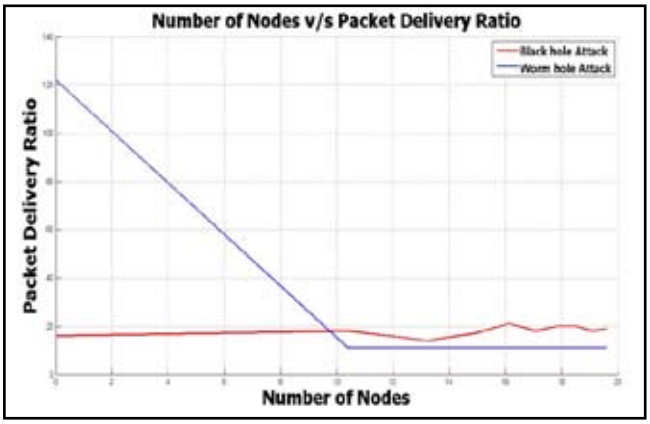

Fig. 6.3: Effect of Attacks on PDR of the network

### A. Routing Protocol Appraoches(AODV, DSDV)

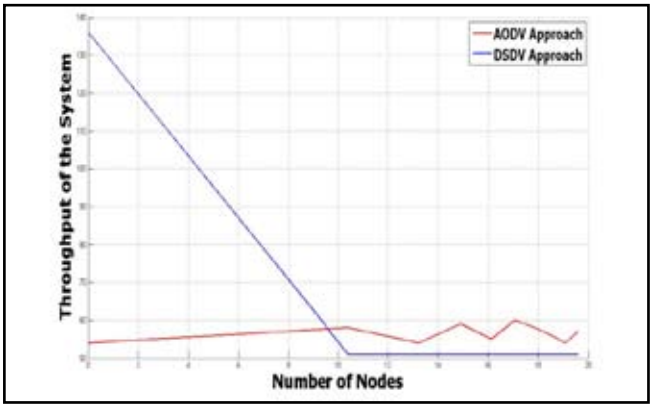

Fig. 6.4 : throughput of the system with protocols

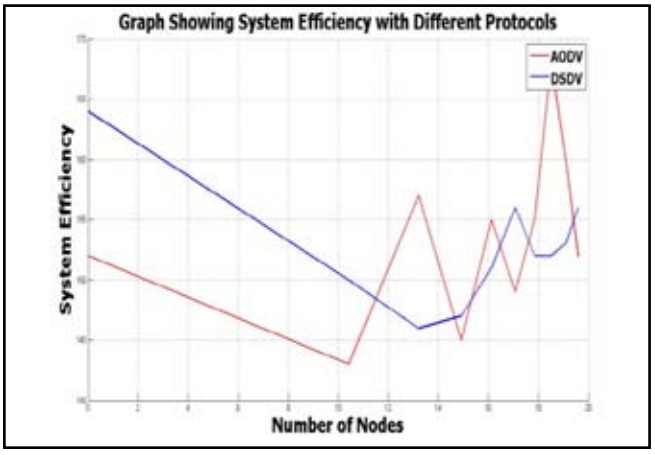

Fig. 6.5 : Comparing AODV & DSDV

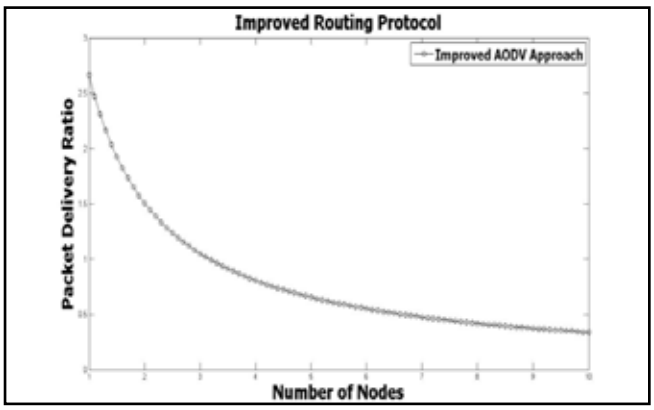

Figure 6.6: Improved AODV

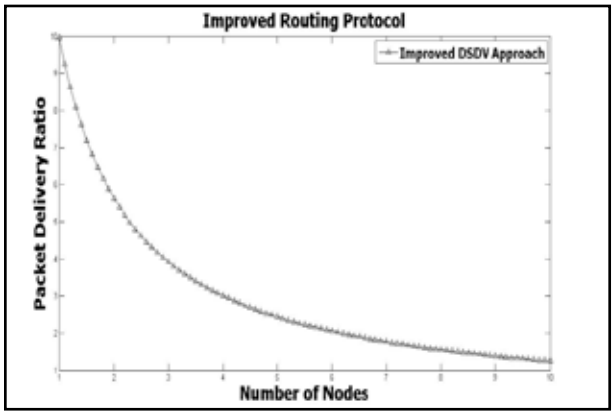

Fig. 6.7 : Improved DSDV

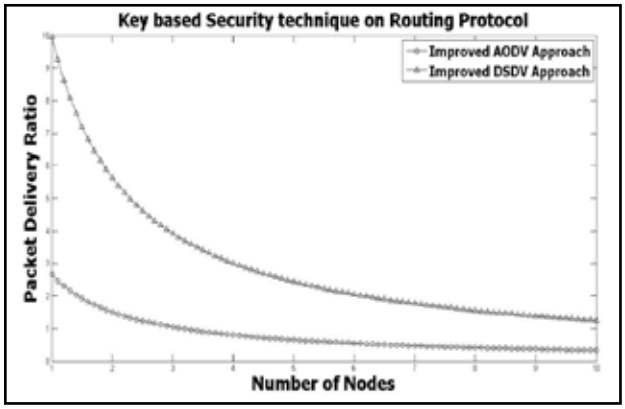

Fig. 6.8: Comparing of Secured Routing Protocols

### B. Overall Comparison

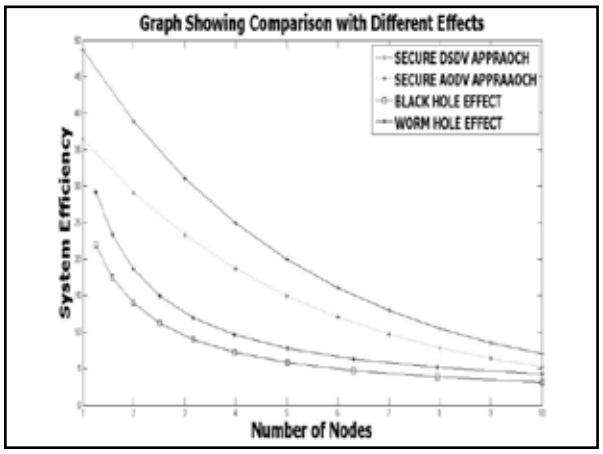

Fig. 6.9: Overall comparison of the system efficiency

## VII. Conclusion

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage.

## VIII. Future Scope

There is a need to analyze Black Hole attack in other MANETs routing protocols such as TORA and GRP. Other types of attacks such as Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research. Further the work can be extended considering more secure environment using different security methods.

## References

[1]. *Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.*

[2]. *Priyanka Goyal,Sahil Batra , Ajit Singh, A Literature Review of Security Attack in Mobile Ad-hoc Networks, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010*

[3]. *Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet Communication , International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).*

[4]. *Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala,A Review of Current Routing Attacks in Mobile Ad Hoc Networks, International Journal of Computer Science and Security, volume (2) issue (3).*

[5]. *Latha Tamilselvan, Dr.V Sankaranarayanan, "Prevention of Blackhole Attack in MANET". The 2nd International Conference on Wireless Broadband and Ultra*

[6]. *Dokurer, S.; Ert, Y.M.; Acar, C.SoutheastCon, "Performance analysis of ad-hoc networks under black hole attacks". Proceedings IEEE Volume, Issue, 22 25 March 2007 Page(s):148 –153.*

[7]. *Chen Hongsong, Ji Zhenzhou, Hu Mingzeng, "A novel security agent scheme for AODV routing protocol based on thread state transition". Department of Computer Science and Technology Harbin Institute of Technology, 150001*

[8]. *Dokurer, S.; Ert, Y.M.; Acar, C.SoutheastCon, "Performance analysis of ad-hoc networks under black hole attacks". Proceedings IEEE Volume, Issue, 22 25 March 2007 Page(s):148 –153.*

[9]. *Fangchao Yin, Xin Feng, Yonglin Han, Libai He, Huan Wang. An Improved Intrusion Detection Method in Mobile Ad Hoc Network, 2009*

[10]. *Dr.Umesh Sehgal, Ms.Kuljeet Kaur, Mr.Pawan Kumar. Security in Vehicular Ad-hoc Networks, 2009*

[11]. *Li-Li PAN. Research and Simulation for Secure Routing Protocol Based on Ad Hoc Network, 2010*

[12]. *S. Albert Rabara, A. Rex Macedo Arokiaraj. IPv6 MANET: An Essential Technology for Future Pervasive Computing, 2010*

[13]. *Yih-Chun Hu, Member, IEEE Adrian Perrig, Member, IEEE, and David B. Johnson "Wormhole Attacks in Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006*

[14]. *Hoang Lan Nguyen, Uyen Trang Nguyen. "A study of different types of attacks on multicast in mobile ad hoc networks". Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008*