ISSN:0975-9646

Robust Security Solution to Countermeasure of Malicious Nodes for the Security of MANET

Kritika Sharma
M.tech(CSE)
Doon Valley Insttitute of Enggineering & Technology, Karnal

Parikshit Singla
Assistant Professor (CSE Deptt.)
Doon Valley Insttitute of Enggineering & Technology, Karnal

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. In this work we have proposed a method to study effect of different attacks on MANET and then analyzed the system efficiency of the network using different routing protocols. Finally the work is extended to countermeasure the effect of these attacks by providing security keys to each node to make them less vulnerable to the attacks. The proposed method is based on the improved routing protocols to increase the system efficiency and security.

Keywords: MANET, attacks, malicious nodes, active attacks, passive attacks.

1. INTRODUCTION

The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes. A Mobile ad hoc network is a group of wireless mobile computers (or nodes). In which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed.

Classification of routing protocols in mobile ad hoc network can be done in many ways, but most of these are done depending on routing strategy and network structure. The routing protocols can be categorized as flat routing, hierarchical routing and geographic position assisted routing while depending on the network structure. According to the routing strategy routing protocols can be classified as Table-driven and source initiated.

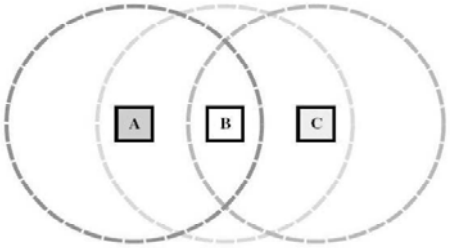

Figure1.1: Example of a simple ad-hoc network with three participating nodes

1.1 AODV PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad-hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources.

1.2 DSDV PROTOCOL

The transmitted routing tables will also contain the hardware address, network address of the mobile host transmitting them. The routing tables will contain the sequence number created by the transmitter and hence the most new destination sequence number is preferred as the basis for making forwarding decisions. This new sequence number is also updated to all the hosts in the network which may decide on how to maintain the routing entry for that originating mobile host. After receiving the route information, receiving node increments the metric and transmits information by broadcasting. Incrementing metric is done before transmission because, incoming packet will have to travel one more hop to reach its destination.

2. LITERATURE REVIEW

S. Albert Rabara, A. Rex Macedo Arokiaraj (2011): This research paper discussed about the technical challenges MANET poses as well as tells about the great opportunities in MANET. The key research issue is to promote the development and accelerate the commercial application of the MANET technology. The main features of IPv6 like security and end-to-end communication are highlighted that are to be integrated with MANET.

S.Tayal, V. Gupta(2013): This paper gives the survey of Attacks on MANET Routing Protocol. MANET is an autonomous system of wireless mobile hosts without fixed network infrastructure and centralized access point such as a base station. Due to lack of a defined central authority, MANETs are more vulnerable to security attacks and thus security is essential requirement in MANET as compared to the wired network. In this paper the authors have attempted to represent an overview of AODV, the possible attacks on MANET and some security mechanism to these attacks.

3. PROBLEM FORMULATION

Previously the works done on security issues i.e. attacks (Black Hole attack) involved in MANET were based on reactive routing protocol like Ad Hoc on Demand Distance Vector (AODV). Black Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how these attacks disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols as well as the impacts of the attacks on the MANETs.

3.1 Security Issues in MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

3.2 Classification of attacks

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack.

3.2.1 External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks. Figure 3.2.1 shows the diagram of external and internal attacks.

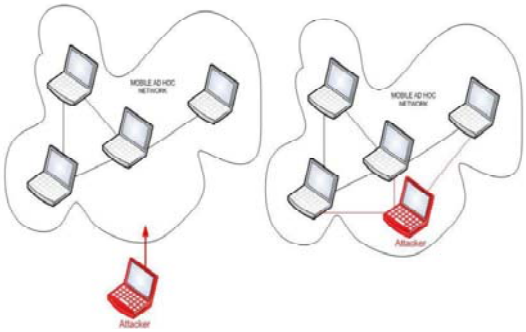

Figure 3.2.1: Internal & External attacks

3.2.2 Active and Passive Attack

When the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network [13]. Active attacks can an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. The figure 3.2.2 below shows the diagram

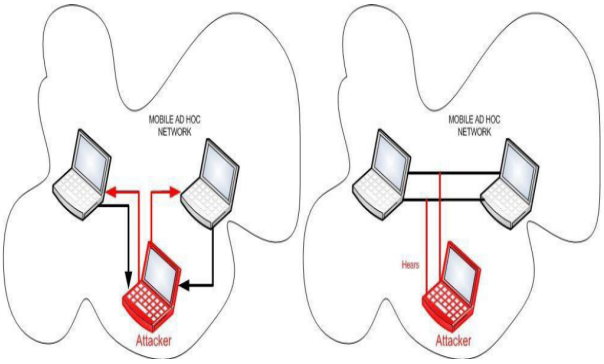

Fig. 3.2.2 Active and Passive Attack in MANETs

3.3 Black Hole Attack in MANET

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

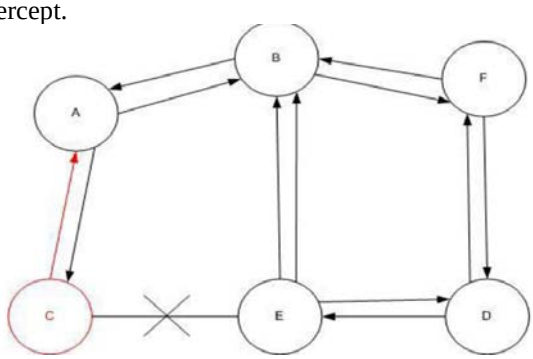

Figure 3.3: Black hole attack

3.4 Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. The fig.3.4 bellow shows the two attackers placed themselves in a strong strategic location in the network.

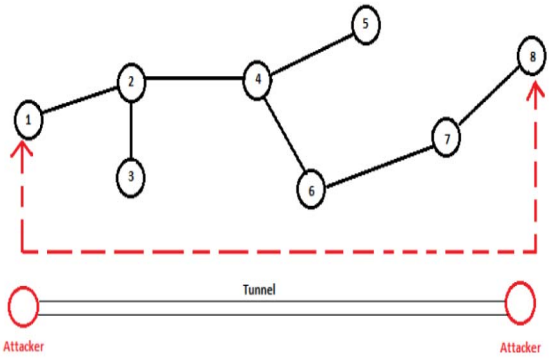

Fig. 3.4: Wormhole attack

In wormhole attack, the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes as shown in the Fig. 3.4 above.

4. PROPOSED APPROACH

4.1.1 Quantitative Approach

This approach is used when the researchers' wants verify the theories they proposed, or observe the information in greater detail.

4.1.2 Qualitative Approach

This approach follows the strategies such as ethnographies, phenomenology and grounded theories. When the researchers want to study the context or focusing on single phenomenon or concepts then they used qualitative approach to achieve their desired goals.

4.2 Our Proposed Method

In our proposed work we have used both quantitative and qualitative approaches. This approach starts by studying the elated literature specific to security issues in MANETs and Manet's literature review is followed by simulation modeling. The results are gathered and analyzed and conclusions are drawn on the basis of the results obtained from simulation. The proposed work contributes the analysis in the graphical form to give a clear comparison between various parameters and techniques.

4.3 Problem Identification and Selection

The most important phase is when, it is important to select the proper problem area. Different areas are studied with in mind about the interest of the problem faced and challenges in the MANET. Most of the time is given to this phase to select the MANET's issue. The proposed work selected MANET as the area of interest and within MANET the focus was given to the security issues and to counter measure the same.

4.4 Proposed Algorithm

```
Algorithm
{
Hop count=0;
Path length =0;
Reachability =0;
For attack node (percentage) =0:1:100
{
For source = 1to N-1
{
For destination= source + 1 to N
{
For iteration 1 to 30
{
Distribute node randomly
If (path exist=y)
{
Calculate
Path length=total distance from S to D ;
Hop count= number of intermediate nodes;
Reachability =reachability+1;
PDR=total packets/total nodes;
Efficiency=delivered packets/available packets;
Simulation time= total distance/speed;
}
}
}
}
Average reachaability=(2*reachability/N(N-1)*25);
AVERAGE PATH length= path length/reachability;
Average hope count=hop count/ reachability;
}
}
```

5. 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 cryptography security keys.

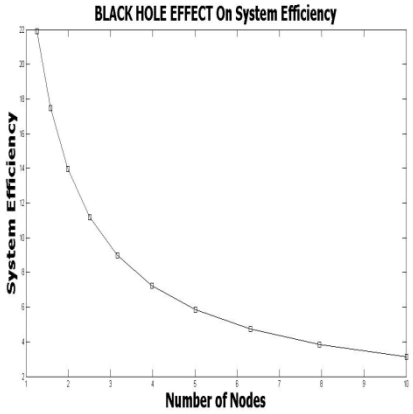

Figure 5.1: Black hole effects on system efficiency

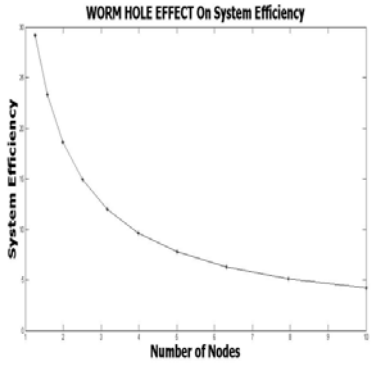

Figure 5.2: worm hole effects on syst em efficiency

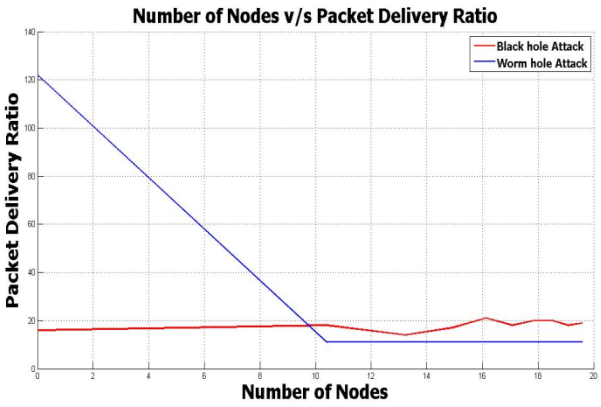

Figure5.3: Effect of Attacks on PDR of the network

5.1 ROUTING PROTOCOL APPRAOCHES (AODV, DSDV)

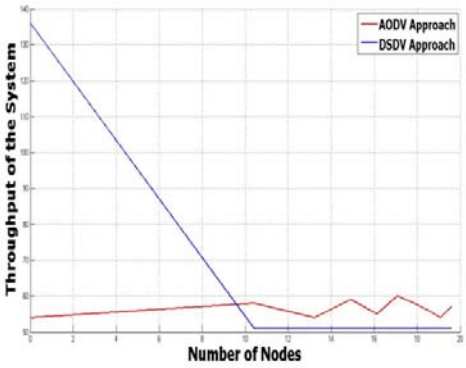

Figure 5.4: throughput of the system with protocols

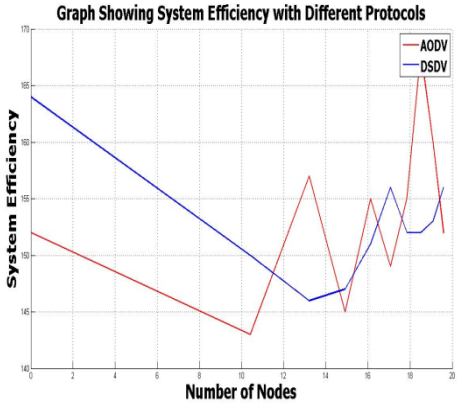

Figure 5.5 Comparing AODV & DSDV

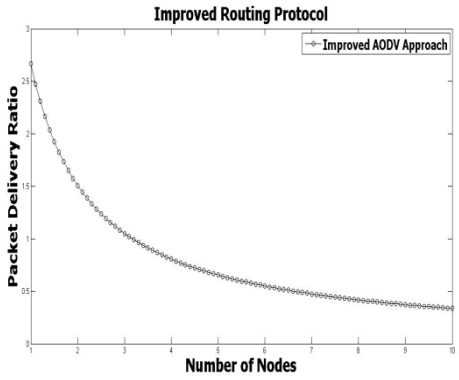

Figure 5.6: Improved AODV

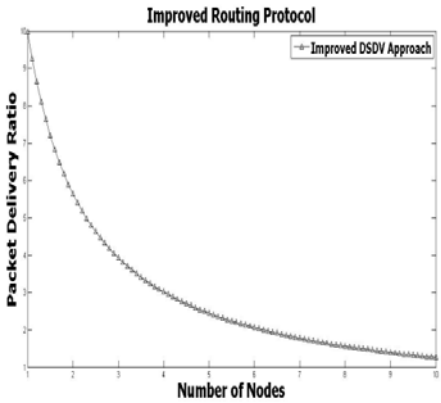

Figure 5.7 Improved DSDV

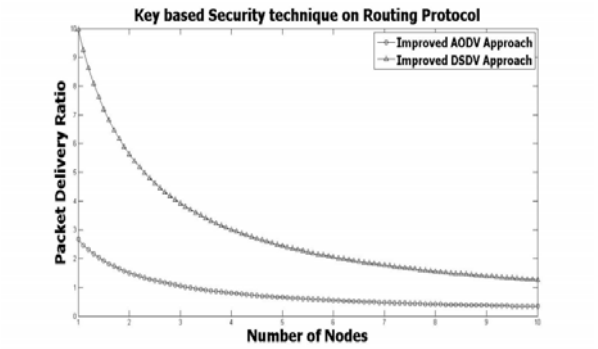

Figure 5.8: Comparing of Secured Routing Protocols

5.2 OVERALL COMPARISON

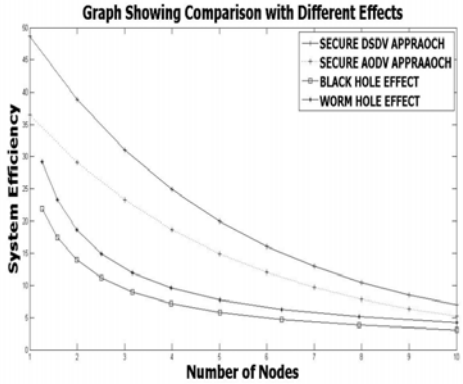

Figure 5.9: Overall comparison of the system efficiency

CONCLUSION

In our proposed work, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding technique using improved routing protocols.

In our study we analyzed that Black Hole attack & worm Hole attack with different scenarios with respect to the performance parameters of end-to-end delay, throughput and network load etc. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols AODV and DSDV have more severe effect when there is higher number of nodes and more route requests.

Finally we have compared the performance of the different attacks with different routing protocols under different parameters.

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] Latha Tamilselvan, Dr.V Sankaranarayanan, "Prevention of Blackhole Attack in MANET". The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) India, 2007 IEEE

[2] 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

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

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

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

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

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

[8] Mohamad Rizal Bin Abdul Rejab, "An Investigation Of TFRC Over MANET Routing Protocol", Universiti Ut Ara Malaysia, 2010.

[9] http://en.wikipedia.org/wiki/

[10] E. M. Royer and T. Chai-Keong, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *Personal Communications, IEEE*, vol. 6, pp. 46-55, 1999.

[11] C. E. Perkins, E. M. Belding-Royer, and S. R. Das "Ad hoc on-demand distance vector (AODV) routing". RFC3561. The Internet Engineering Task Force, Network Working Group, Jul2003.http://www.ietf.org/rfc/rfc3561.txt.

[12] http://www.ece.iupui.edu/~dskim/manet/

[13] Kavitha Kumar, "Intrusion Detection in Mobile Ad-hoc Networks", University of Toledo, 2013.

[14] http://en.wikipedia.org/wiki/Personal_area_network, last visited 12, dec, 2013.