

DETECTING GREYHOLE & BLACKHOLE ATTACK USING IDEA CRYPTOGRAPHY IN MANET

VenkataMounika Namburi¹, Sisir Bolisetty², Saketh Krishna Velugoti³, T N Shankar⁴

^{1,2,3,4} Department of Computer Science and Engineering, K L University, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India.

¹mounikanamburi04@gmail.com

Abstract: Development of a secure MANET in real scenario is an insipid task which involves in a secured design with reduced level of energy consumption. It is necessary to operate over the continuous node processing system, as mobile nodes are resource constrained. The major attacks in a wireless MANET are black-hole & grey-hole. Black-hole & Grey-hole attacks are related to network layer that spoil the entire network by falling-packets. In Black-hole attack, the false nodes are unable to provide the correct path within a group of nodes to the receiver nodes during routing process. The attacker attains such type of attacks where all of the similar kinds of nodes transmit data to another. The responsibility of the MANET is to protect network layer from various types of attacks. An advanced secured cryptographic model is essential to defend such type of malicious elements. Detection of grey-hole and black-hole attacks can be addressed in MANET with accuracy by using such type of technique. IDEA is the best to implement as an advanced cryptographic model with the better security level within the limited energy constraint.

Keywords — MANET, IDEA, cryptography, Security, Wireless network, Black-hole attack.

1. Introduction

The MANET (Mobile Adhoc Network) refers to the multi-hop packet of wireless network made out of ambulant nodes which can convey and move at a same time, by unusable type of wired framework [1].

MANET is a well-organized and adaptable framework which is formed without any incorporated association. A MANET is abbreviation of Mobile Adhoc network that location can be changed and designed on the fly.

These are portable to use with the remote alliances by the interface of different systems.

The occasion of MANET working set is to get a standard internet routing protocol utility that's appropriate for any mobile routing application inside both stable and active topologies which expands to a vital range because of node motion and different elements [2]. The methodologies are consciously lightweight in nature and suitable for various hardware in portable situations to address the scenarios where MANETs are conveyed to the boundary of an IP groundwork. Hybrid mesh work is a framework that must be upheld with MANET's determinations and management factors. Utilizing full-fledged components on the test WG will create two standard track routing protocol specifications: Reactive MANET Protocol (RMP) and Proactive MANET Protocol (PMP) [4]. Some attacks are obstacle for data transmission in MANET. Black-hole attack, Denial-of-service attack (DOS), Grey-hole attack, Jelly fish attack are major among them. In this paper IDEA cryptography technique is employed for data security which detects the black-hole & grey-hole attacks. IDEA Cryptography is a symmetric by nature. It has better resistance command over differential cryptanalysis technique which makes utilization of different group of operations to raise its quality against usual recognizable attacks. IDEA comprises of 128 bit of key that provides a better security. No direct or algebraic attack has been efficient to break key within a stipulated time. The process applies to all keys can divide IDEA in 6 rounds.

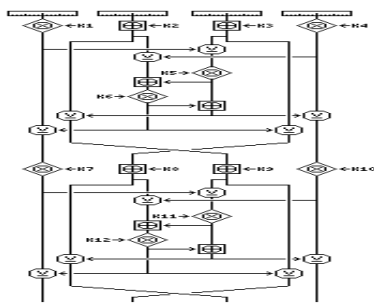


Figure 1. Idea Cryptography Structure

In IDEA Cryptography both encryption and decryption are similar. Different operations are performed to achieve the higher level security. Operations in IDEA cryptography are as follows:

- Bitwise exclusive OR operation..
- Addition modulo of 2^{16} .
- Multiplication modulo of 2^{16+1} .

This will be helpful in data transmission by availing better security to thwart the defined attacks.

2. Related Work

Marti et.al have discussed two methods to improve throughput in Adhoc network that accepts packet forwarding. To overcome this issue, arrangement of nodes are based upon dynamically calculated behavior. Utilization of watchdog to identify malicious node and a path rater so as to aide's routing protocol maintain a distance from these nodes. Through reproduction we evaluate guard dog and way rater by utilizing bundle throughput, rate of the overhead (steering) transmission and exactness of pernicious hubs [1].

Watchdog and path rater are ascertained by utilizing packet throughput, rate of overhead (steering) transmissions. Throughput is expanded by 17% within the sight of 40% acting up nodes and the rate of overhead transmissions from the standard steering convention's increments from 9% to 17%. Amid outrageous portability, throughput is expanded by 27% and overhead transmissions from the standard directing convention is 12% to 24%.

Marchang focused on Mobile Adhoc networks (MANETs) are initially intended for supportive environment. To utilize this network in the present environment, trust based routing can be used to find the trusted route, instead of searching for the shortest path using various routing algorithms. Light-weight intrusion detection protocol is used to estimate the trust between the nodes and also utilize less computational resources. This protocol deals with two sort of attack: black-hole attack and the

grey-hole attack. This protocol is incorporated in any routing networks [2].

Khalil's sleep-wake protocols are predominantly utilized as a part of sensor systems to guarantee broad process. In some situation, problem occurs in creating an effective mechanism that would incorporate with sleep-wake protocol for both extensive procedure and high safety. To address this issue native observation can be used as an intense method for detecting data attacks in sensor network [3].

Each and every node has some traffic regulations going through its neighbors to find-out the suspicious behavior. Unusually delay in sending a package is the instance of it. To overcome this problem a protocol named SLAM is proposed to observe the energy consumption and organization of it with sleep-wake protocol in WSN. The assessment to authorize sleep-wake in a secured way even in face of node that might be opposed. Simulation process is carried out in ns-2 to exhibit the performance and energy consumption is reduced.

D. B. Johnson discussed that an informal system is a collection of wireless portable hosts determining a temporary network of any well-known framework or unified organization. It is vital for a host to locate the neighbor hosts in transmitting packets from source to destination.[4] A dynamic routing protocol is proposed in this paper. This protocol is adaptable according to the changes in frequency. Based on the simulation, the performance of this protocol is good at various environments. For all except the maximum rates of host movement simulated, the overhead of protocol is very low by falling to only 1% of aggregate information package transmitted in a system of 24 portable hosts [5].

3. Existing System

Present black-hole Resisting Mechanism (BRM) is used at various on-demand routing protocols. Each and every node of this mechanism was accountable for observing the behavior of its neighbors to detect malicious nodes and eliminate them. They Integrate the mechanism into an on-demand Ad-hoc routing protocols like Ad hoc on-demand distance vector (ADOV) [6]. The mechanism introduces a different method that clarifies the detection of a malicious invader. It is adapted by obeying with the regular

protocol bearing and attract the harmful node to provide implicit about the malicious behavior.

4. Proposed System

A mechanism is proposed with IDEA cryptographic technique for finding the major attacks in the MANET. This technique is useful to detect black-hole & grey-hole attacks precisely. RREP report is used to know whether the node is neighbor or not [7]. At first the median node executes IDEA cryptographic algorithm. It calculate the proceeding metrics of the malicious node and contrast them against other RREP. If routing responds is violated then that node is said to have grey-hole node. The outcome demonstrates that the strategy gives both higher throughput and preferable conspiracy resistance over the current techniques. There is no current places of business on false information for various straightforward attack situations. This accounts a grey-hole attack by traded off nodes in a way that utilizes abnormal information aggregation.

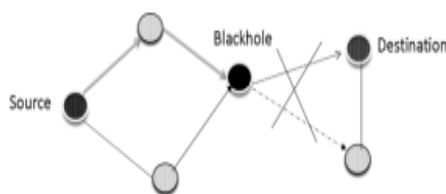


Figure 2 Black-hole attack

Topology Creation

During simulation fifty numbers of detector nodes are deployed. They are randomly sent with a size 2000 X 1500. Poisons process is used at every sensor for generating data packets which are having same parameter of low traffic load to compute a feasible system situation. We set a speed go from max 5 m/s to min 2.70 m/s. The nodes will have an transaction range of 250 m and a data rate of 50 kbps. The size of the packet is controlled by size of information payload and by space required to incorporate the data of the next hop forwarder set. We assume that the information packet has drift of 150 bytes.

Black-hole /Grey-hole Attack

Black-hole attack occurs during the transmission of information between the nodes in the routing layer.

The most important thing that happens in the routing layer is transmission and dropping of packets. As communication is done in the routing layer, routing protocol has a threat of attacks. This attack has tremendous effecting strike on implicit network. Denial-of-service (DOS) comes under this attack as it does not provide any further communication. It is hard to identify this attack as most part is found in temporary networks like virtual/remote work systems.

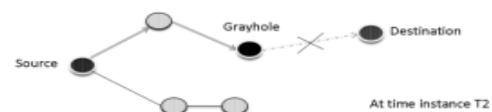
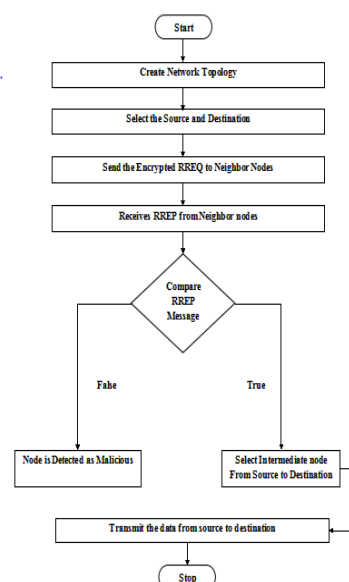


Figure 3 Grey-hole attack



Grey-hole attack will have an impact on the execution of mesh network. The source node receive reply from the authorized node that provides a short path to destination and malicious node reply to the sender that the data is received. Source gets confused with two replies. The malicious node gets to be the sender node and the whole data is received by it. During this process the information packet totally dropped by the source. The sender node sends RREQ messages to every neighbor node and that request is taken by malicious node.[8] The harmful node pretend to have the shortest path to the receiver node which

in turn not a real path. At that point sender node recognizes the sent reply from malicious node and exchange the data.

5. Result Analysis

NS2 Tool is used for the simulation purpose in this paper. It has the ability to delivers partly and provides free source code which can be modified and expanded easily. Comparison is done between the existing method (self-trusted mechanism in MANET) and proposed method (IDEA cryptography). The difference in the throughput can be observed by using the graphs acquired from the simulation.

The Black-hole attack has an impact during the packet transport that can be observed in Figure 4. Black-hole attack has an extreme effect on AODV as it has the uniquely substantial number of harmful nodes.

A graph is obtained from the simulation, which has throughput on X-axis and number of black holes on Y-axis. Red line on the graph shows the existing work and green one shows the proposed work. The throughput of IDEA mechanism is better than BRM-AODV.



Figure 4. Network throughput for black-hole

The effect of Grey-hole attack during packet transmitted to the destination can be shown in the figure. The graph obtained has Time on X-axis and Network_NQW on Y-axis. The proposed system is successful in getting numerous data from source to destination node. It varies the original node from malicious node and provide safe path between the nodes.

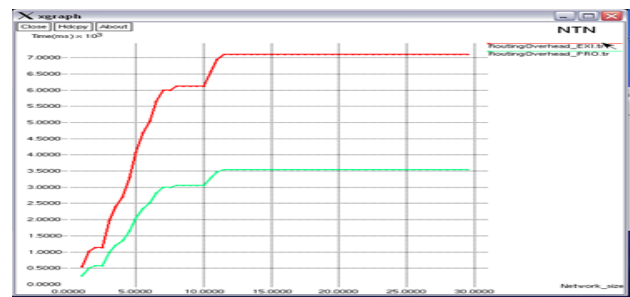


Figure 5 Network throughput for grey-hole

6. Acknowledgment

In this project the work that is proposed is supported by T.N.Shankar, suggested us to use symmetric cryptography technique for more security, for detecting authenticated nodes and for less consumption of energy.

7. Conclusion

The concept of security with IDEA is better for communication. A secured cryptographic model using idea cryptography is discussed in this work. This concept can be employed in network protocol design for establishment of secure connections among the existing nodes. Energy utilization is the most vital part among the nodes in communication system. The intention of the paper is to efficiently use for all mobile nodes at the reduced level of energy consumption without compromising the security level. The paper is meant for detecting and reducing grey-hole and black-hole attacks with more accuracy. Finally, the results are simulated and carried out in NS2 simulator.

References

- [1] S. Miarti, T. J. Giiluli, K. La and M. Bakerer, "Mitigating steering Misbe-havior in a transportable Adhoc atmosphere," Proc. 6th Annual ACM/IEEE International Conference on portable compute and network, pp. 255-265, August 2000.
- [2] N. Marchang, R. Datta, "Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks," IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.
- [3] S. K. Bhreoi and P. M. Khilarai, "Vehicular statement: examination", IET system journal, vol. 3, no. 3, 2014.
- [4] Hiren Sharma, PrativaRai, BhupeshDeka "Energy efficient Communication Protocol for

Wireless Sensor Network with mobile node”, IEEE conference, Recent Advances and Innovation in Engineering, Jaipur, India 9-11 May 2014

[5] Praveen kumar.J , Ezhumalai.G,”interactive web design with security based 2-factor authentication”,International Innovative Research Journal of Engineering and Technology, vol.1,no.3,pp.23-28, 2016.

[6] R. Hunt, A. Hassan, and S. Zeadally, “Vehicular ad hoc system (VANETS): category, effect, and dispute,” Telecommunication Systems journal, vol. 50, no. 4, pp. 217-241, 2012.

[7] C. Manikopoulos and L. Ling, “building of the transportable Ad hoc complex sanctuary (MANS) structure,” Proc. IEEE International symposium on Systems, gentleman and Cybernetics journal, vol. 4, pp. 3122- 3127, October 2003.

[8] K. Nadkarni and A. Mishra, “interference recognition in MANETs – The following divider of security,” Proc. IEEE commerce Electronics humanity consultation journal, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.

[9] Mohamed A. Abdelshafy, Peter J. B. King, “Resisting black hole attack in MANET”, 13th IEEE Annual Consumer Communications & Networking Conference journal, 2016.

