ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 6, June 2015

A Research Study on Sinkhole Attack in Mobile Adhoc Networks and Signature Based Algorithm

S. Mohamed Imranul Hasan

Research Scholar ,Deparment of Computer Science,Sri Krishna Arts And Science College,Coimbatore.

Dr.V.Radhika

Principal,Sri Krishna Aditya Arts And Science College,Coimbatore.

Abstract— **The Mobile Ad hoc Network is a most important and popularly used communication Network Now days in the modern wireless based communication System. This Mobile communication network is structure less network which operations are mainly depend on the nodes that act as a blood vessels of this Mobile Ad hoc Network. The Major attack faced by this network is sinkhole attack which can heavily attract the resources available in the network towards it. It has to be prevented to make the energy of the network is available for all resources. The Signature based algorithm is the commonly used to know the masquerade attack that has a large impact on the data tampering.**

***Index Terms*—MANET.**

I. Introduction

In this research paper we focus on the sinkhole attack that attracts all the available resources in the standard structure less mobile ad hoc network. We also have a elaborate look on the signature based Algorithm to prevent illegal data packet tampering on the Mobile Ad hoc Network. These Security Attacks has to observe in detail and the solution and Methods to avoid and get rid from these attacks in mobile Ad hoc Network has to be devised and formulated.

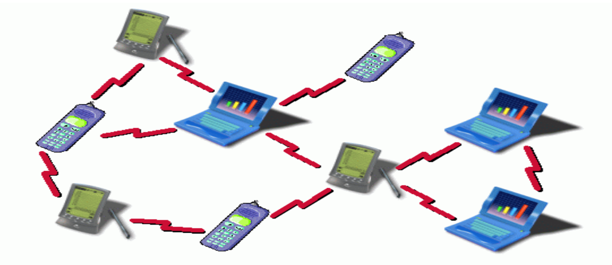
II. Literature Survey

A. *Ad hoc Network*

The Word Ad-hoc which is commonly used today originates from a Latin word, which means "for this purpose ". The Most Popular Ad-hoc network is an self operable networks that can be deployed anyplace and anytime without the need of a large and costly infrastructure. It is used for military oriented purposes.

B. *Mobile Ad-hoc Network (MANET)*

A mobile ad hoc network (MANET) is an combination of a group of continuously self-configuring, infrastructure-less network of movable devices connected without the help of wires. Each and every device in a MANET is free to move independently in any direction, able to communicate with each other and will therefore change its links to other devices frequently. Each and every device that is communicating within the mobile ad hoc network must exchange traffic unrelated to its own use, and therefore each device act as a router. The major and more important aspect and challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.



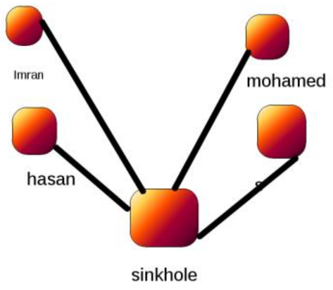
In the above depicted figure both the laptops and cell phones exchange information’s among themselves. They use configuration less communication gateways to establish connection among themselves. In mobile Ad hoc Network various types of telecommunication devices communicate among them.

III. SINKHOLE ATTACK

The sinkhole attack in the mobile ad hoc network is most deadly attack when compared to all the other attacks in the mobile Ad hoc network.

A. *Sinkhole Attack Structure and Operation*

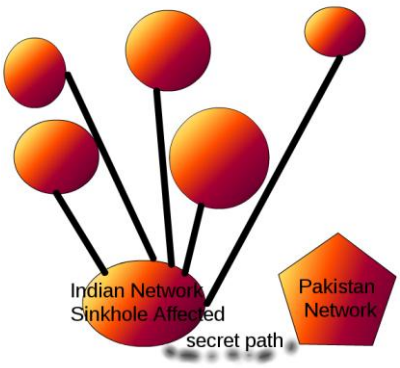
The sink is a place where all the content flows. It is a common method where used in our wash basins. All the content will flow towards it. Almost same like that the sinkhole attack can attract all the data traffic towards it in the mobile Ad hoc Network. The Structure of the Sinkhole attack in the mobile Attack Network is stated below.



There can be a simple communication path between the nodes hasan and mohamed which is simpler and much cost effective one. But this Sinkhole node in the mobile ad hoc network causes a sinkhole attack; it means it makes all the data transmission to be established through that node only. By this feature the sinkhole node can get access to all the data exchanged among all the other nodes in the mobile Ad hoc network.

B. *Threat for Security*

Since this sinkhole node act as a super node and through which all the connections are happening. If this node is accessed are attacked all the important and most secure information's of the nodes in the mobile ad hoc network can be accessed. Since the mobile ad hoc network are deployed in each and everywhere. It is most suited communication system used in the Warfield and security areas by our defense forces.



For a simple example consider a situation where are mobile ad hoc network system used by the Indian De fence forces has a sinkhole attack. And all the military secrets are passed by the sinkhole present in the Communication System. If that sinkhole is accessed by a wormhole attack.In that all the military communication will be accessed by the Pakistan defense forces. All the Military secrets of India will be leaked. This will cause a big security threat to India. So It is a impact of the sinkhole attack. The Secret path is the constructed using the another attack available in the mobile ad hoc network is wormhole attack which is a process of establish a secret path in the mobile ad hoc network and making the information's to flow to some other predefined location

C. *Sinkhole Prevention*

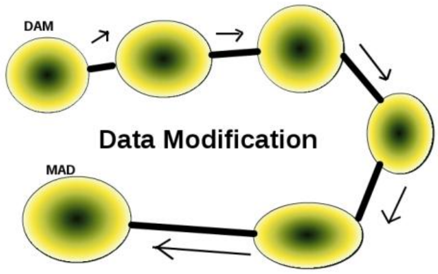
The Sinkhole attack has to prevent by a proper security methods and this information's has to be kept secure. It can be done using a signature based algorithm or behavior based algorithm through which the most optimal path are calculated and routing protocols through which these data are transferred.

IV. SIGNATURE BASED ALGORITHM

The Signature based algorithms are used to encounter the most deadly attract that is Masquerade or Data tampering Attack.

A. *Operation and Power*

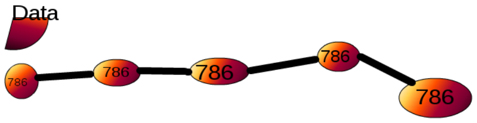
Since the mobile ad hoc network is most commonly dependent on the nodes available in the mobile ad hoc network for communication. Each and every nodes can get access to a data till it reaches the destination. There arises a problem that the vulnerable node can easily access and even modify the data sent through them.



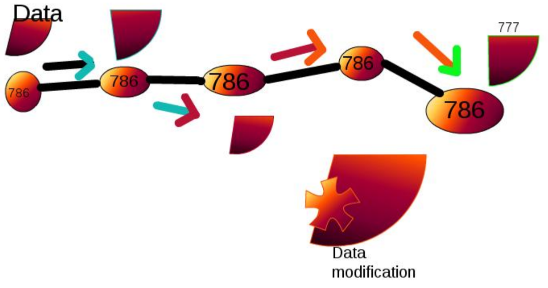
For Example, we are sending a data to "DAM" from the first node to a 100 Th node. During the transmission operation the data is accessed and modified and finally the data received by the 100 th node is "MAD". If the most trusted information has to be exchanges and if that happens. It will question the operation of the network..

B. *Use of Signature Based Algorithm*

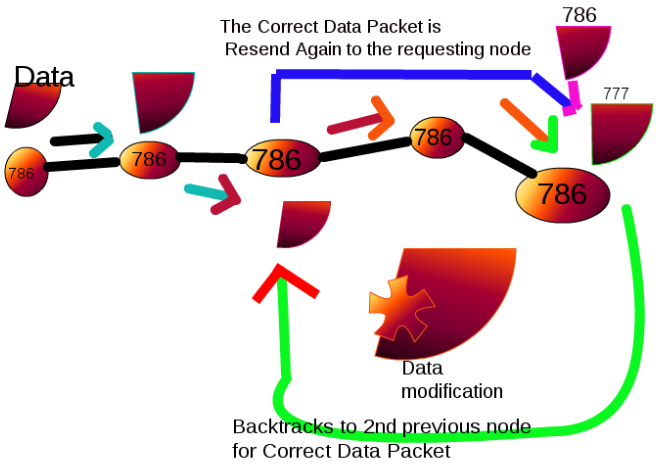
In order to solve and overcome the problem of data tampering/masquerade and modifications, we use the concept of signature based Algorithm.In order to identify the nodes which tampers and modifies the data packets that are being transferred along them? I have analyzed and to set a predefined threshold value for each node and if the data are tampered and modified and the threshold value will be changed .Based on the changes in the predefined threshold value that particular node can be avoided in the communication for the next time. For Example We want to transfer the data "Prophet Mohamed (Sal)" among the nodes in the mobile ad hoc network. My Research idea and proposal is to assign all the nodes in the mobile ad hoc networks a predefined threshold value "786" before the exchange of data among the nodes.



When the operation begins each and every nodes in the mobile ad hoc network will data packet if it is send without opening and modification their threshold value will not be changed .If the packet is opened their predefined threshold value will be incremented by 1.And that threshold value will be embedded to the packet and passed to another node.



The node receiving the modified packet from the security threat node will compare its threshold value with the threshold node valued in the packet if it is not correct. It will discard that packet and will back track to the second previous node to get the correct data and it passes to the destination.


The Correct Data Packet is
Resend Again to the requesting node
786
777
Data
786
786
786
786
786
Data
modification
Backtracks to 2nd previous node
for Correct Data Packet

V. Conclusion

This research paper focused on the sinkhole attack that is present in the mobile ad hoc network. We also had an elaborated analysis on the signature based algorithm and its operations. Thereby paving a way for secure communication between nodes in Mobile Ad hoc Network. Through the continues work we can find or completely overcome the threat for the mobile ad hoc network. In future Research this can be used to make the data transmission on MANET as more reliable one.

Acknowledgment

The word "Acknowledgment" is the most respectable way to express our gratitude to those who backed us in all our endeavors. I thank my parents, family members, friends and all our teachers. I thank the Almighty who creates and protect us all.

REFERENCES

[1] Security Issues in MANET: A Review. Mahakal Singh Chandel,Arjun Institute of Advaced Studies and Research Centre, Indore,India. Rashid Sheikh, Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, India,2010 IEEE.

[2] Security Architecture for MANET and It's Application in m Governance,Baljeet Kaur, Bharati Vidyapeeth Deemed University, Pune. Institute of Management and Entrepreneurship Development. 2013 International Conference on Communication Systems and Network Technologies.

[3] T. H. project, "Know your enemy," July 2000. [Online].Available: http://project.honeynet.org/papers

[4] E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks", book published by Wiley, 2009.

[5] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Commun. Surveys and Tutorials, vol. 8, num. 2, pp. 2–23, 2006.

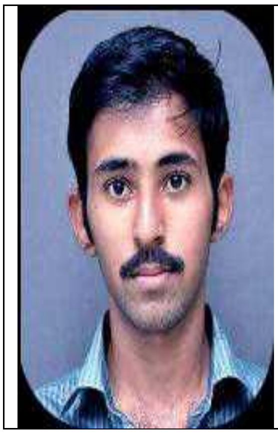
[6] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International J. Computer Science, vol. 4, num. 1, pp. 1–9, 2009.

[7] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems", Elsevier J. Information Security Technical Report, vol. 10,num. 3, pp. 134-139, 2005.

[8] I. Butun and R. Sankar, "A Brief Survey of Access Control in Wireless Sensor Networks," in Proc. IEEE Consumer Communications and Networking Conference, Las Vegas, Nevada, January 2011.

[9] M. Ngadi, A.H. Abdullah, and S. Mandala, "A survey on MANET intrusion detection", International J.Computer Science and Security,volume 2, number 1, pages 1-11, 2008.

[10] Y. Zhang, W. Lee, and Y.A. Huang, "Intrusion detection techniques for mobile wireless networks", J. Wireless Networks, vol. 9, num. 5,pp.545-556, 2003.



He received his bachelor degree in Computer Applications, from Bharadhisan University; Trichy in 2011.He received his Master Degree in Computer Applications. From Anna University, Chennai in 2014.He is doing his research degree in Computer Science from Bharathiar University, Coimbatore. He hails from Coimbatore.

Radhika.V received her B.Sc (Phy) ,MCA and M.Phil degree from Bharathiar University Coimbatore. in 1993 ,1996 and 2003 respectively. She received her PhD from Avinashilingam university for women,Coimbatore. in 2013. She is the Principal,Sri Krishna Adithya Arts And Science College , Coimbatore. She has 18 years of teaching experience. She has more than 25 publications at national and International level.