Spoofing – An attack on node identity and its Remedial Research

A. Udhaykumar, M Ganesh Raja

ABSTRACT---Network is the prime demand of today's outreaching development in every sector. Starting from a small institute to big sectors like Industry, Organization, Defense, Ministry and Medicine all are dependent on network to maintain their data transmission efficiently. It provides the great ease of operation and information sharing. As we know with greater ease, much greater threat is handy. With the network also a big threat is associated i.e. network attacks. There are some major attacks which can violate and damage the whole network system and its integrity. Wireless attacks are very common and an intruder with vast knowledge of network administration and modification can easily find the loopholes in the security systems. There are different attacks like Denial of Services (DoS), Sniffer, Password Based, Spoofing, Eavesdropping etc. but the most dangerous of all is spoofing. Spoofing is an attack type in that the intruder impersonates as original identity and use their identity to achieve the intrusion goal. The attack is so severe because the user, even after seeing the intruder cannot identify it as the external body and take immediate action. The intruder enters the network and steals all the information as a legitimate user and damages the integrity of network. We propose here to find the intruder by using the energy consumption by nodes using the dead, asleep and active nodes. We can localize the location of intruders in the network using this technique. We use Received Signal Strength (RSS) to see the energy consumption of each node as the fluctuation of intruder node will be different from genuine nodes.

Index Terms: Received Signal Strength (RSS), Denial of Services (DoS), Sniffer, Password Based, Spoofing, Eavesdropping

I. INTRODUCTION

India, after the introduction of Digital India concept has suddenly become a country of digital advancements. Free Wi-Fi on Railway Stations, Bus Stands, Airports and different public places are quite common. One who connects to these networks show their MAC address unknowingly to the service providers. A person with little effort can find the MAC address of the network sharers and enter in their peripheral end devices. Then stealing the information is way easier. All the information are a material to acquire is available handy with the intruders. Then the question comes. Why the service providers not bother to create a system to protect the users against those threats? The

Immediate reason of this negligence is overhead cost and need of R&D. Generally username and password based authentication and sometimes even the One Time Password (OTP) is considered the full proof system against threat in Indian Wi-Fi networks. Our work is to analyze the present scenario and check the probability, remedy and conclusion of the spoofing attack in Indian networks. At first we discuss about the need of the implementation followed by the tools and the technique to solve the issue.

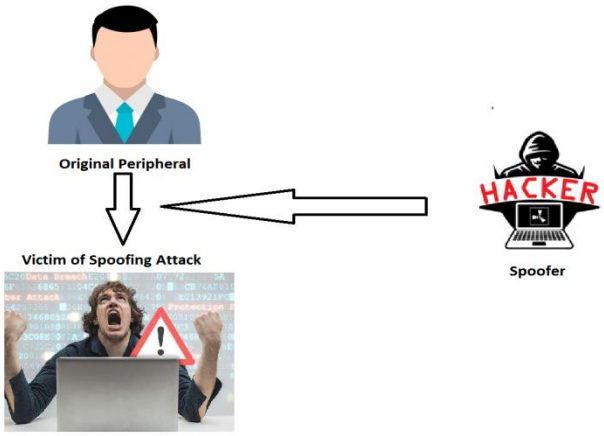


Fig. 1.1 – Spoofing attack scenario

The Received Signal Strength (RSS) is the prime technique in our system to find the intruding node. The node acquiring inadequate levels of signal is the black sheep in the network. We first create the node topology and then apply node weight and assign priority index to check the packet transmission. It's like the scenario of real-time network where we check the asleep, dead and active node to interrogate the impact of the attack. We also plot the graph for the packet loss vs energy graph as the validating point for our proposed approach. In our next section we thoroughly read several related literature surveys and their correlation with our proposed approach.

II. LITERATURE SURVEY

Kamal Kumar Chauhan and Amit Kumar Singh Sanger paper was about the efficient management of keys and much authenticated routing protocol in which the group leader has all the authority to maintain the key. They can generate and spread the key in as secure away it's possible. Every time a new node wants to enter the group it needs the authentication by the group leader then only it can mix with other nodes in the network.
It can also maintain the stability of nodes by protecting the information available in the packets. The auto reply system also is analyzed by the group head as the double authentication system. [1]

Yong Sheng3, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell explained how a spoofer can enter the network and damage he whole system by tricking wireless service points and advertise the fake services in the network. The Received Signal Strength (RSS) is a system which is very hard to falsify and can catch the intruder node. The

Revised Manuscript Received on 14 August, 2019.
Dr. A. Udhaykumar,
M Ganesh Raja,

distance of the intruder and the node being attacked are on certain distance then the criteria fulfilling the received signal strength can differentiate and notify about the spoofing and Man in the Middle Attack. RSS is the received strength of the frame at the receiver's end. It is highly dependent on the power with which the signal was transmitted, the distance between the transmitter and receiver and most important the path or channel it uses. The path might have less or more interference which leads to the different received signals. [2]

Yingying Chen, Wade Trappe, Richard P. Martin discussed that compared to previous systems of the spoofing detections like the key based systems this is much easier due to its lower overhead. They developed and implemented K-means spoofing detector. They used dual algorithms to detect the point and area. The false detection rate was approx. 5% which is actually a very good score of such systems. They mentioned their system can be implemented with different types of the networks and algorithms so it is highly efficient and easily implementable. They plotted the graph for estimated distance from localization vs True distance between two nodes which validated their result. They have done the centroid in the signal transmission/reception range is a good factor for the node reliability. The position of attacker can be localized easily in this system. [3]

III. IMPLEMENTATION PHASE AND METHODOLOGIES

Different steps to launch the spoofing detector were carried out. We discuss all the phases in detail in the following paper. As the architecture diagram states that we first develop the network by using the appropriate topology. The assignment of weight for the node is done. The asleep and wake nodes are selected from the group of the nodes and the overall nodes are checked. The nodes which are active in state are checked for current node states otherwise again the nodes are checked to meet active node condition. The energy and packet loss graph is generated to analyze the result. This scenario provides the clear picture of the overall working model. The data transferred and the nodes consuming the data are checked for the Received Signal Strength (RSS). The graph is plotted to show the energy drop per packet. This graph shows the scenario which is the replica of real-time system.

A. Architecture Diagram

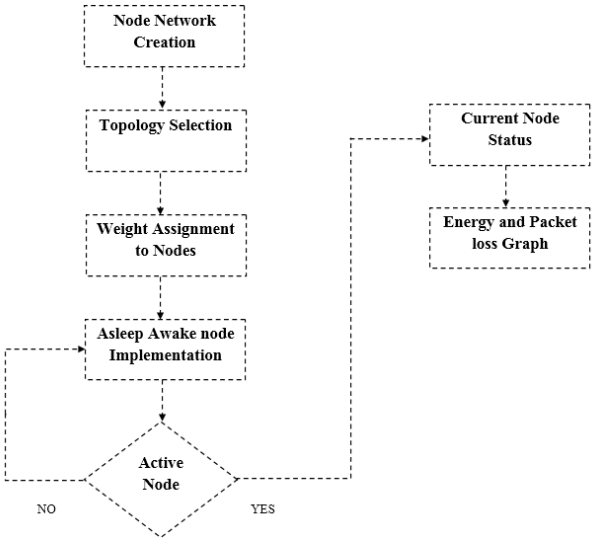


Fig. 1.2 – Architecture Diagram

B. Sequence diagram

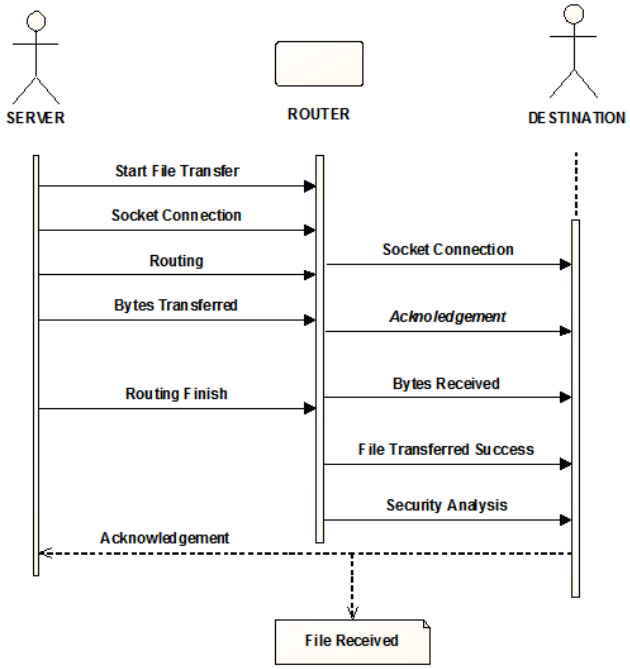


Fig. 1.3 – Sequence diagram

The sequence diagram represents that a source and destination is available for the data packet transmission. There is a router available to move the packet in the correct route. At first the file transmission starts. The system checks whether the socket connection is available or not. If the socket connection is available then the routing connection is established. The socket connection is established between Server Router and Router Destination. Then the byte transfer occurs and based on efficient socket connection the data transmission takes place.

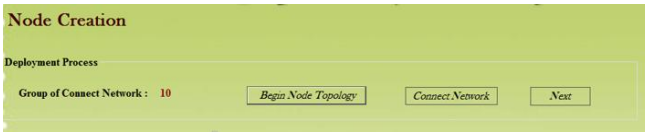
The file is transferred successfully. The security analysis is the main part of work we do. We check the nodes available are of genuine category based on Received Signal Strength (RSS). The acknowledgement is then checked for

genuine transmission of data. This guarantees the service and the quality of data transmission/reception.

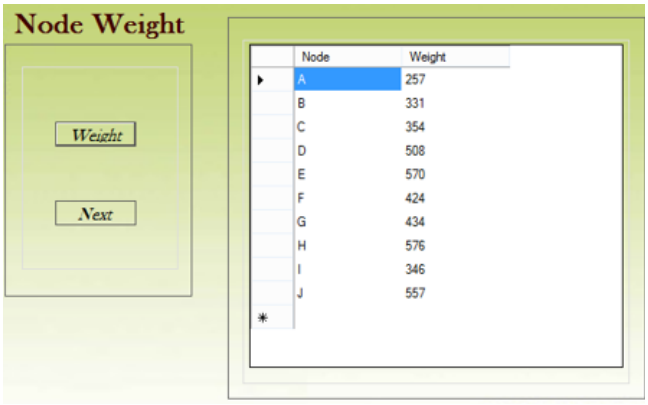
IV. IMPLEMENTATION AND OUTPUT & RESULTS

i. Node Creation

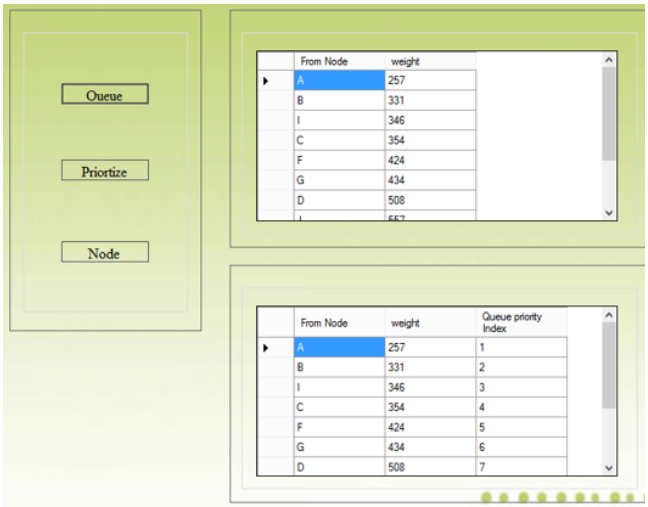
ii. Group of connected networks selection



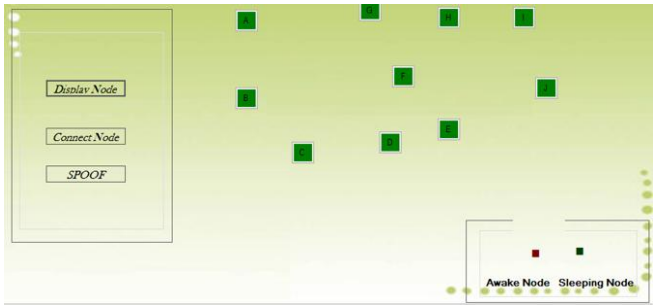
iii. Node weight assignment



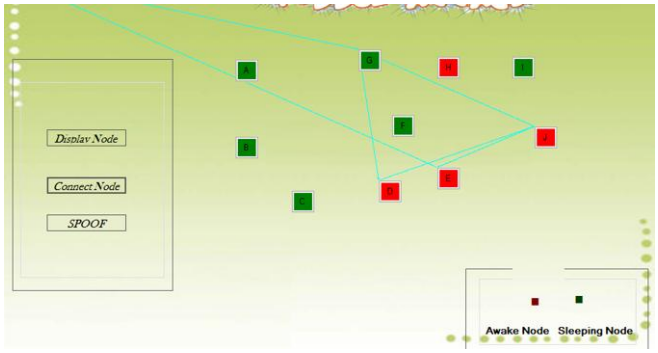
iv. Set priority for each nodes



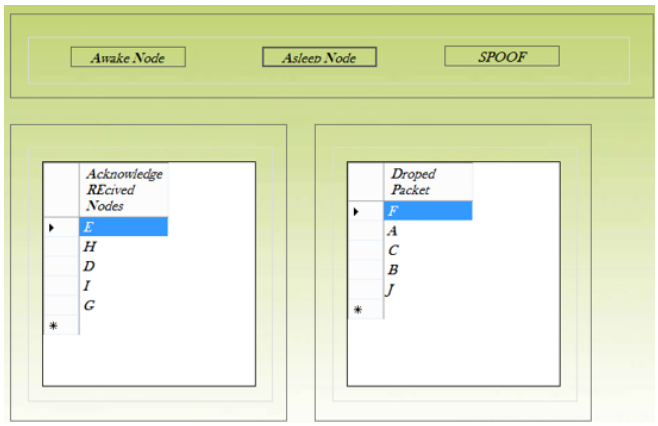
v. Invoke Attack



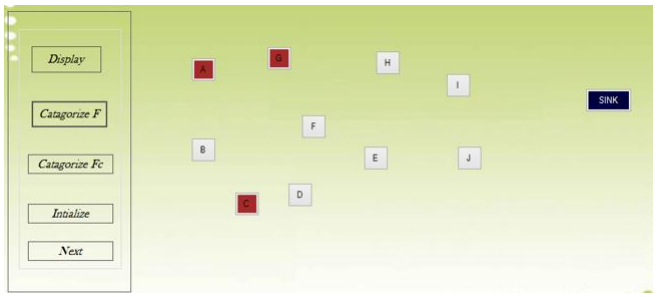
vi. Attack response



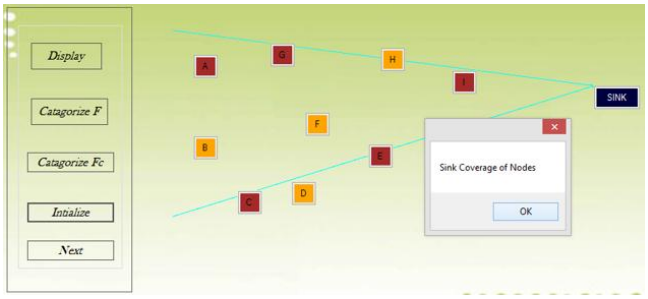
vii. Inter Domain Packet Filters



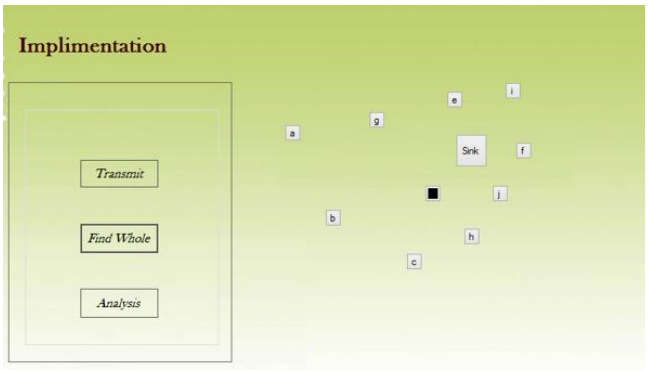
viii. Positive and Negative Nodes



ix. Spoofing Implementation



x. Communication among the nodes



xi. Packet Validation

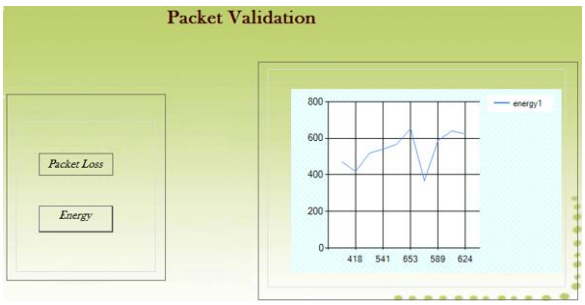


Fig. 1.4 – Result Graph 4

V. CONCLUSION AND FUTURE ENHANCEMENT

This research paperdiscussed theimmediateeffects,parameters, evaluations and consequences of spoofing attack. Different possible solutions implementation and results. We implemented the Received Signal Strength (RSS)-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. In future we can increase the efficiency of detecting the attacker and also we have to drop the attacker level actions.

REFERENCES

1. Kamal Kumar Chauhan and Amit Kumar Singh Sanger, "Securing Mobile Ad hoc Networks: Key Management and Routing" in International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.
2. Yong Sheng, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell1, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength" in IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, May 2008
3. Yingying Chen, Wade Trappe, Richard P. Martin," Detecting and Localizing Wireless Spoofing Attacks" in 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks.
4. B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS), 2006.
5. P. Bahl and V. N. Padmanabhan, "Radar: An in-building rf based user location and tracking system," in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), March 2000, pp. 775–784.
6. M. Youssef, A. Agrawal, and A. U. Shankar, "Wlan location determination via clustering and probability distributions," in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom), Mar. 2003, pp. 143–150.
7. E. Elnahrawy, X. Li, and R. P. Martin, "The limits of localization using signal strength: A comparative study," in Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004), Oct. 2004, pp. 406–414.
8. W. A. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 network has no clothes," IEEE Wireless Communications, vol. 9, no. 6, pp. 44–51, Dec. 2002

AUTHORS PROFILE

Dr A. Udhayakumar has graduated in Bsc, Computer Science from Bharathidasan University in 2003 and also Post graduated in Msc, Computer Science from the same Bharathidasan University in 2005. After getting his Master Degree, he studied M.Phil from Alagappa University in 2009. He earned Ph.D., degree in Computer Science from Karpagam University in 2017. He is presently works as Assistant Professor in the Department of Computer Science at Agurchand Manmull Jain College, Meenambakkam, Chennai, Tamil Nadu, and India. He specialized in Network Security and Cryptography of Mobile Computing. He contributed as author and co-author for more than 40 papers in Computer Science and technical journal conference proceedings, author of UGC NET PAPER-I Teaching and Research Aptitude and UGC NET COMPUTER SCIENCE PAPER-II and APPLICATIONS. He also honoured the best paper award for various conferences. He cracked UGC NET (National Eligibility Test) two times and SET (State Eligibility Test) and Many MOOC (Massive Open online Course).

M.Ganesh Raja received the Bsc, and MCA, degrees in Computer Science fromPondicerry University in 2008 and 2011, respectively. He received the M.Phil degree in Computer Science from University of Madras in 2015. He is currently working as a Assistant Professor with the Department of Computer Applications in AgurchandManmull Jain College, Chennai, Tamil Nadu, India.