INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 5 May 2016.

A REVIEW PAPER TO DETECT AN ISOLATE ATTACK IN WSN AND PROVIDING SECURITY USING RSA AND MD5 ALGORITHMS

Swati Mehta [a,*], M.D. Umar [b], Kapil Mangla [c]

[a,b,c] Satya College and Technology, Haryana, India

ABSTRACT

The increase of the technology revolution is encouraging WSN to be used in different sectors and for different purposes. These sensor node are used for collecting and sending data and transmit among the networks. Each node can move freely in any direction, and changes their links to other devices frequently. Security is an essential part of Wireless Network. Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole and gray hole attack is one of them. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. Where it is easy for an attacker to physically capture some of the legitimate nodes, copy credentials, reprogram them and re-deploy them in the WSN. Such type of attack is called Node Replication or Misdirection Node Attack. With this attack an attacker can easily gain significant control over the WSN. Basically, this mechanism provide the security of RSA and Md5 algorithm in WSNs.

Keywords: Wireless sensor network, black hole, multiplebase station etc.

I. INTRODUCTION

A wireless sensor network (WSN) consists of large numbers of sensor nodes, which are consistent through wireless links to perform distributed sensing task. These sensor nodes collect data from the network and report to the sink. The sink node is one of the very critical elements of the wireless sensor networks (WSNs). In the future the sensor networks will be widely use with the help of promising sensing and wireless technologies. These technologies can be deployed in civil or military applications. Sensor network are often used in application where it is difficult to setup wired network for example, monitoring in wild life, military surveillance and tracking objects.

To protect important information researchers in sensor network have focused on finding way to provide good security services such as (CIA):

- Confidentiality

- Integrity
- Availability

Black hole and Gray Hole Attack

WSNs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized as:-

Black Hole Attack: In this type of attack, one malicious node uses routing protocol to claim itself of being shortest path to destination node but drops routing packets and doesn't forward packets to its neighbours.

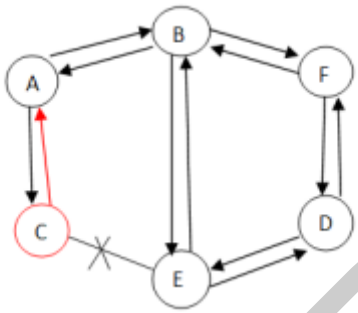

Fig. 1: Black hole Attack

Gray Hole Attack: The gray hole attack is also a kind of DoS attack. Gray hole is an extension of black hole attack in which malicious node behaviours and activities are exceptionally unpredictable. In this, malicious node advertise a same behaviour as a authentic node during route discovery process and silently drops some packets or also forward packets even when no congestion occurs. This malicious node degrades the network performance that disrupts the route discovery process. This attack is difficult to detect than black hole attack.

II.LITERATURE REVIEW

A **literature review** is a text written by someone to consider the critical points of current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work. Also, a literature review can be interpreted as a review of an abstract accomplishment

H. Deng [1] proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If the black hole nodes work as a group in an attempt to drop packets, then this method is not efficient.

Mohammad Al-Shurman [2] proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. When the source node receives RREP packets and the routes to destination have shared hops, the source node can then recognize the safe route. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. This mechanism is reliable and faster having no overhead.

Latha Tamilselvan [3] proposed the solution in which the source node waits for the responses including the next hop details from other neighbouring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table) table, whether there is any repeated next-hop-node or not. If any repeated next-hop node is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited. The solution adds a delay and the process of finding repeated next hop is an additional overhead.

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan [4] provide an improvement over the solution given in the paper in which Source Intrusion Detection (SID) method is used. The SID mechanism is good for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is long, then the above solution is not sufficient. Secondly, if the distance between the source node and the intermediate node is long, the delay in the discovery period of the route will be high, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

III.WSN CHALLENGES

A WSN environment has to overcome certain issues of limitation and inefficiency. It consists of following:

- **The characteristics of wireless link are time-varying in nature -** There are transmission barrier like path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The dependability of wireless transmission is resisted by different factors.
- **Limited range of wireless transmission -** The limited radio band results in reduced data rates compared to the wireless networks. Hence best usage of bandwidth is necessary by keeping low overhead as possible.

- **Packet losses due to errors in transmission** - WSNs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER), interference, and frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and unidirectional links.
- **Route changes due to mobility-** The dynamic network topology results in frequent path breaks.
- **Frequent network partitions**- The random movement of nodes often leads to partition of the network. This usually affects the intermediate nodes.

IV. SECURITY TECHNIQUES

RSA AND MD5

These two algorithms start with the unique set S taking it the main node. Every iteration of the algorithm means in each step, it iterates through each unused attribute of the set S and calculates the entropy $H(S)$ (or information gain $IG(A)$) of that attribute. Then selects the attribute which has the smallest entropy (or largest information gain) value. The set S is then split by the selected attribute (e.g. age < 50, 50 <= age < 100, age >= 100) to produce subsets of the data. The algorithm continues to recurse on each subset, considering only attributes never selected before.

Recursion on a subset may stop in one of these cases:

- Every element in the subset belongs to the same class (+ or -), then the node is turned into a leaf and labelled with the class of the examples
- There are no more attributes to be selected, but the examples still do not belong to the same class (some are + and some are -), then the node is turned into a leaf and labelled with the most common class of the examples in the subset
- There are no examples in the subset, this happens when no example in the parent set was found to be matching a specific value of the selected attribute, for example if there was no example with age >= 100. Then a leaf is created, and labelled with the most common class of the examples in the parent set.

Throughout the algorithm, the decision tree is constructed with each non-terminal node representing the selected attribute on which the data was split, and terminal nodes representing the class label of the final subset of this branch.

➢ RSA is an assymetric encryption algorithm. You have two keys (private and public) and you can perform a function with one key (encrypt or decrypt) and reverse with the other key. Which key you use depends on whether you are trying to do a digital signature or an encryption.

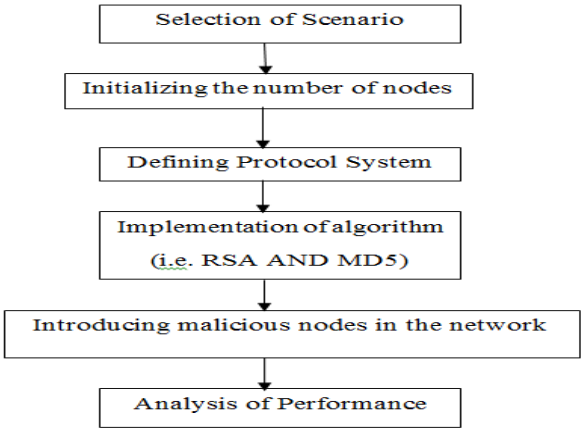

Fig. 2: Work Flow

➢ MD5 and SHA are hash functions (SHA is actually a family of hash functions) - they take a piece of data, compact it and create a suitably unique output that is very hard to emulate with a different piece of data. They don't encrypt anything - you can't take MD5 or SHA output and "unhash" it to get back to your starting point. The difference between the two lies in what algorithm they use to create the hash. Also note that MD5 is now broken as a way was discovered to easily generate collisions and should not be used nor trusted anymore.

V.CONCLUSION

A Wireless Sensor Network(WSN) is composed of a group of mobile, wireless nodes which cooperate in forwarding packets in a multi-hop fashion without any centralized administration. In this research work is done on the security of WSNs. Firstly scenario is created then nodes are initialised then for the implementation RSA AND MD5 is used which detect the black hole and grey hole attack which is type of DOS attack.

ACKNOWLEDGMENT

Working on this thesis **to detect an isolate attack in WSN and providing security using RSA and MD5 Algorithms** provided a unique experience and analysis, I feel great pleasure and privilege in working over this research. I am deeply indebted to **" Satya College of Engineering and Technology "** for the invaluable guidance, support and motivation for the many other aids without which it would have been impossible to complete this project. I have no words to express my deep sense of gratitude for MD.Umar (Mentor) sir for his enlightening guidance, directive encouragement, suggestions and constructive criticism for always listening to our problems and helping us out with their full cooperation. Last but not the least, Father Lajpat Mehta Mother Harsha Mehta who have given me that much strength to keep moving on forward every time, we are greatly thankful to them and have no words to express my gratitude to them.

REFERENCES

[1] C. E. Perkins and E. M. Royer,"Ad-hoc on-demand distance vectorrouting. In Proc. 2nd IEEE Workshop on Mobile Computing Systemsand Applications", Vol.3, pp. 90–100, Feb. 2012.

[2] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in WSN Routing Protocol",International journal Computer Technology & Applications,Vol.3, Issue 6,pp. 1915-1921, Nov-Dec 2013.

[3] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in SecureWSN" Vol.2, Issue 2,pp. 15-21, 2012.

[4] H. Tian and H. Shen, "Multicast-based inference of network-internalloss performance," in Proc. of 7th International Symposium on ParallelArchitectures, Algorithms and Networks , Hong Kong, China, Vol.6 pp. 288–293, May 2011,.

[5] IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.2, No6, December 2014.

[6] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Vol. 3, Issue 5, May 2013 ISSN: 2277 128X.

[7] J. Liebeherr, J. Wang, and G. Zhang. Programming overlay networkswith overlay sockets. In Proc. 5th COST 264 Workshop on NetworkedGroup Communications (NGC 2003), LNCS 2816,Vol.7,Issue 4 pp. 242–253, Sep.2013.