AD-HOC Chief Spoofing Forestall In Wireless Sensor Networks

[1]G.C.Jagan, [2]Sharon Stella.R, [3]Sushmitha.U, [4]Swetha.D

[1]Assistant Professor, [2,3,4]Students,
Department of Electronics and Communication Engineering,
Jeppiaar Engineering College, Chennai, India.

Abstract: **Wireless spoofing attacks are easy to launch, it plays a significant role in the performance of wireless sensor networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. The challenging tasks in Wireless Sensor Network are identification of spoofing attackers, determination of number of attackers, localization of multiple adversaries and eliminating them. The clustering approach is used to detect the spoofing attackers and localize them. This approach fails to predict the attackers accurately. To overcome this problem, proposes Intrusion Detection System (IDS) to detect the spoofing attackers. Watchdog timer that automatically generates a system reset if the main program neglects to periodically service it.OTCL language is used for simulation. Linux (*Ubuntu*) is used as the operating system. Network Simulator 2 is a simulation tool for Linux. The simulation result clearly shows that the proposed scheme detects the spoofing attackers in Wireless Sensor Network efficiently and robustly.**

Index Terms: AD-HOC wireless sensor networks, NS2 simulator, NAM tool

I. INTRODUCTION

A wireless ad hoc network (WANET) or mobile ad hoc network (MANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use.

II. ANOMALY DETECTION

2.1 Network Coding

The next-generation network is network coding because it can maximize the throughput capacity of a network. By using NC, nodes in the network can encode and decode the received data packets instead of only store and forward. When the encoding and decoding are linear operations on a finite field, it is called linear network coding (LNC). For multiple multicast, LNC has been applied to improve the transmission throughput. Related studies have proved that LNC not only can make the multicast transmission reach the theoretical upper bound of throughput but also can provide information confidentiality due to its inherent characteristics. Specifically, when applying LNC to multicast communication, the data information transmitted in the network is no longer the original data chunk, but the linear combination of original data chunks, which is called the encoded packet. If the attacker cannot receive enough encoded packets, it cannot obtain information about the original data chunk. In this condition, LNC becomes an effective way to resist passive attacks and provide secure data transmission without the key distribution protocols, which reduces the system complexity .In order to provide data confidentiality, existing researches mainly focus on two different security requirements: Information Theoretical Security (ITS) and Weak Security (WS).ITS requires that any nonzero linear combination of original data chunks cannot be obtained by attackers. In order to achieve ITS, random information must be added to encode together with original data chunks during data transmission. On the other hand, WS does not allow any meaningful information, e.g., the coded packets that can be generated by the original data packets of the same data stream be leaked to the attacker. It is noted that the data stream means a data flow in which all the data are collected by the same sensor.

2.2 Linear Network Coding

Network coding is a field of research founded in a series of papers. However, the concept of network coding, in particular, appeared much earlier. paper a scheme for improving the throughput of a two-way communication through a satellite was proposed. In this scheme, two users trying to communicate with each other transmit their data streams to a satellite, which combines the two streams by summing them modulo 2 and then broadcasts the combined stream. Each of the two users, upon receiving the broadcast stream, can decode the other stream by using the information of their own stream. The 2000 paper gave the butterfly network example (discussed below) that illustrates how linear network coding can outperform routing. This example is equivalent to the scheme for satellite communication described above. The same paper gave an optimal coding scheme for a network with one source node and three destination nodes. This is the first example illustrating the optimality of convolutional network coding (a more general form of linear network coding) over a cyclic network. Linear network coding may be used to improve a network's throughput, efficiency and scalability, as well as resilience to attacks and eavesdropping. Instead of simply relaying the packets of information they receive, the nodes of a network take several packets and combine them together for transmission. This may be used to attain the maximum possible information flow in a network. It has been mathematically proven in theory that linear coding is enough to achieve the

upper bound in multicast problems with one source. However linear coding is not sufficient in general (e.g. multisource, multi sink with arbitrary demands), even for more general versions of linearity such as convolutional coding and filter-bank coding. Finding optimal coding solutions for general network problems with arbitrary demands remains an open problem.

2.3 Encoding and Decoding

In a linear network coding problem, a group of nodes are involved in moving the data from source nodes to sink nodes. Each node generates new packets which are linear combinations of earlier received packets, multiplying them by coefficients chosen from a finite field, typically of size.

$$X_k = \sum_{i=1}^{S} g_k^i \cdot M_i$$

where the values are the coefficients selected from. Note that, since operations are computed in a finite field, the generated message is of the same length as the original messages. Each node forwards the computed value along with the coefficients, , used in the level . Sink nodes receive these network coded messages, and collect them in a matrix. The original messages can be recovered by performing Gaussian elimination on the matrix. In reduced row echelon form, decoded packets correspond to the rows of the form.

III.PROPOSED SYSTEM

Here Neural Networks based controller to send the data to the observer is implemented. On sending data, some attacks are occurred at intermediate nodes and Adaptive Dynamic Programming (ADP) method is used to implement the attacks and on other intermediate nodes. For time varying, it shows that how much time it takes such that time delay and also the analysis of performance on a throughput is made.

3.1. Hybrid Routing Protocol

Hybrid Routing Protocol (HRP) is a network routing protocol that combines Distance Vector Routing Protocol (DVRP) and Link State Routing Protocol (LSRP) features. HRP is used to determine optimal network destination routes and report network topology data modifications

3.2. Watchdog Timer

A watchdog is a device used to protect a system from specific software or hardware failures that may cause the system to stop responding. The application is first registered with the watchdog device. Once the watchdog is running on your system the application must periodically send information to the watchdog device

IV.RESULTS

In Fig 4.1. the ranges of each node in the network region has been assigned. The packets can reach the destination from the source through these intermediate nodes. To pass it to the intermediate nodes, the source node has to check whether its immediate neighbour node is within the proper range, inorder to carry the packet to the correct destination.

In Fig 4.2. Malicious node has also been assigned. Once the malicious node been found, the watchdog timer act as an reagent and passes the packet through other nodes to destination using hybrid protocol.

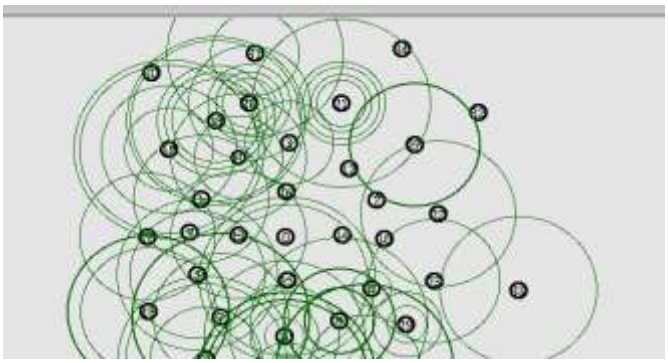

Fig.4.1. Range of each nodes

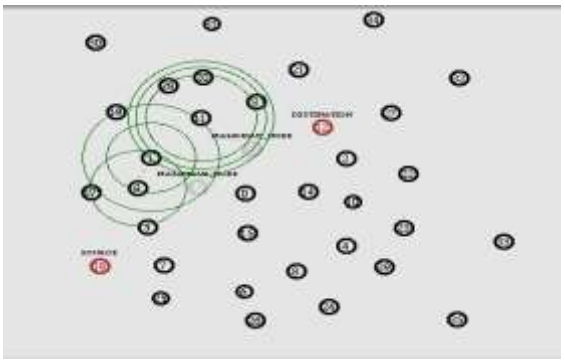

Fig.4.2.Creation of watchdog timer

As a result of doing this, it is noted that the throughput, how much data can be transferred from one location to another in a given amount of time, has considerably increased from the existing system which can be clearly seen in Fig 4.3.a. From Fig 4.3.b. the parameter namely, Packet Delivery Ratio, the ratio of number of packets delivered in total to the total number of packets sent from source node to destination node in the network, has considerably increased from the existing system.

From Fig 4.3.c. the parameter namely, Delay, the latency for a bit of data to travel across the network from one communication endpoint to another, has notably decreased from the existing system.

Finally, it is noted that the energy is also consumed less which can be noted in the Fig.4.3.d.

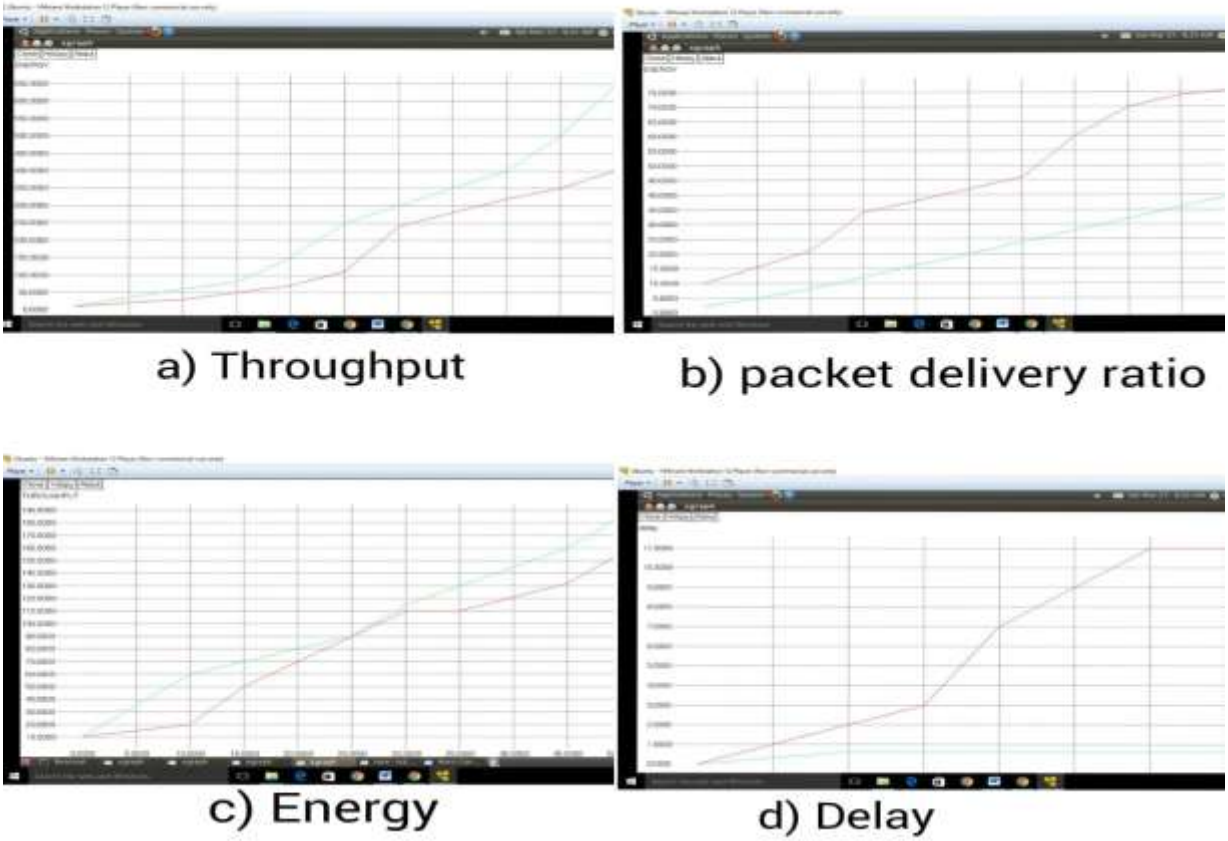

Fig.4.3.Parameter Measurement

V.ACKNOWLEDGEMENT

We would like to express our sincere thanks to our supervisor Prof.G.C.Jagan for assisting us in the project. We would also like to thank our college for the support. Last but not the least we would like to extend our gratitude to our families for constantly supporting us throughout the project.

REFERENCES

1. A. Giorgetti, M. Lucchi, E. Tavelli, M. Barla, G. Gigli, N. Casagli, M.Chiani, D.Dardari .(2016) " A robust wireless sensor network for landslide risk analysis". IEEE Sensors Journal, 16(16): 6374-6386.
2. N.P. Ju, J. Huang, R.Q. Huang, C.Y. He, Y.R., Li. (2015) " A Real-time monitoring and early warning system for landslides" Journal of Mountain Science, 12(5):1219-1228.
3. M. Li , Y.H. Liu. (2007) " Underground structure monitoring with wireless sensor networks".6th International Symposium on Information Processing in Sensor Networks (IPSN'07), Cambridge, MA, USA, pp. 69-78.
4. A. Rosi, M. Berti, N. Bicocchi, G. Castelli, A. Corsini, and M. Mamei. (2011) " Landslide monitoring with sensor networks: Experiences and lessons learnt from a real-world deployment". International Journal of Sensor Networks, 10(3):111-122.
5. W. Z. Song and R. Huang. (2009) "Air-dropped sensor network for real-time high-fidelity volcano monitoring". Proceedings of the 7th international conference on Mobile systems, applications, and services (MobiSys'09), Kraków, Poland, pp. 305-318.