

An Efficient Fuzzy Logic Comparison with Different Method in MANET

V. Navamani¹ Dr. P. Radha²

¹Research Scholar ²Assistant Professor

^{1,2}Department of Computer Science

^{1,2}Government Arts College (autonomous), Coimbatore – 18, Tamilnadu, India

Abstract— The Mobile ad-hoc network (MANET) is a moveable wireless network that can transfer the information from source to destination; this network is widely used all around the wireless network because it does not require any fixed wired network to establish communication between the source and the destination. In this research paper we take MANET as a main passive attack in such as Sybil node based on the parameters of the node and also uses two bio metrics as the key values of data encryption and decryption is detected and the result is compare with respect to the parameter.

Key words: Fuzzy Logic, MANET

I. INTRODUCTION

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the on-going communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DOS), selfish node misbehaving, impersonation attack is kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. ALGORITHM AND PARAMETER FOR MANET

A. Fuzzy-Logic

The rules are as follows:

- 1) If whole data is adequate or required data value is small then Security is low.
- 2) If whole data is marginal and required data value is large then security is normal.
- 3) If whole data is inadequate then security is high.

B. Membership Function

The network parameters can take a dynamic range of values based on various locations on the network. In the proposed work, the input parameters are normalized to hold values. Later during fuzzification, crisp normalized values are

converted into fuzzy variables. For this, three fuzzy sets have been defined for each variable.

C. Sybil Attack Detection using Fuzzy Logic

To identify the Sybil attack, the Sybil Attack Detection Algorithm (SADA) with fuzzification method is proposed; it is utilized to separate the Sybil node and the legitimate node even if it has the highest mobility through the verification process. The AHIDS absorbs each node RSSI value in the table with respect to the time period, and it analyzes whether the first RSSI value is lesser than threshold or not. If not, AHIDS includes it to the attacker list and updates its neighbours list.

The proposed SADA is combined with the rule based anomaly detection module. In this mechanism, the anomaly detector utilizes fuzzy rules set to differentiate data units as normality or anomalies. While supervising the WSN, these fuzzy rules sets are chosen appropriately and employed to the supervised data. If the fuzzy rules are satisfied in determining, an anomaly is announced. The ASADA, the underlying detector, is compiled into four processes, towards observing Sybil attacks in the wireless sensor networks. In this first process, nearby nodes identify the path for the data transmission, utilizing the range-enabled scheme which sends hello packets to the neighbor nodes (which are also called beacons). The data packets are utilized within the particular range in order to receive the effective RSSI signal; if they cross a certain distance or range, then the signal strength becomes weaker which has the possibility of getting affected by the malicious nodes, so the ranging estimation scheme is included. In this scheme, each packet has the PHY header (PHR) with particular bit which is called the ranging bit; moreover, each packet broadcasts the PHY for the frames sets meant for ranging.

III. RESULT AND DISCUSSION

In Biometric based Sybil attack detection method, the nodes are detected as Sybil nodes based on fuzzy logic and biometric Authentication. Its security level is high when comparing with Light weight Sybil attack detection method and Robust Sybil attack detection method.



Fig. 1: Image watermarking using DWT for Security

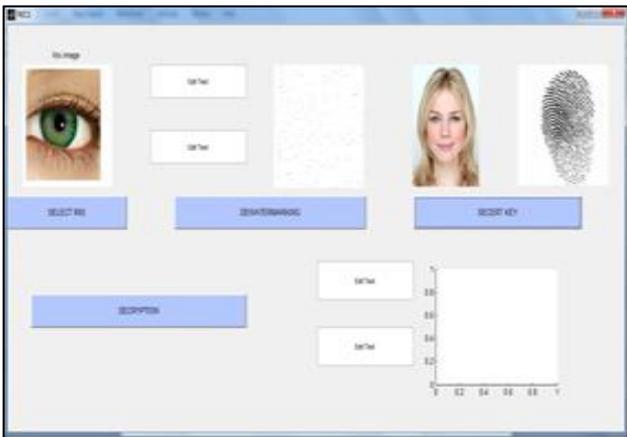


Fig. 2: Secret Key (Face and Fingerprint) Selection for Decryption

IV. CONCLUSION

In this research paper MANET is implemented with different methods, algorithm using speed, time, and energy. After evaluate all the method fuzzy logic has better performance when compared with Robust Sybil attack Detection Method and Biometric based Sybil attack detection method. This research can further extended using modify neural network algorithm.

REFERENCES

- [1] R. Amuthavalli, Dr. R. S. Bhuvaneshwaran, "Detection And Prevention Of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method", 2010
- [2] K. Hoepfer and G. Gong, "Bootstrapping security in mobile ad hoc networks is using identity-based schemes," in Security in Distributed and Networking Systems Singapore: World Scientific, 2007.
- [3] S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010.
- [4] Y. Chen, J. Yang and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans. Veh. Technol., Jun. 2010.
- [5] M. S. Bouassida and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET,"
- [6] RenXiu -li, Yang Wei, "Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network", 2009 IEEE.
- [7] Tamilarasan Santhamurthy, "A Comparative Study of Multi-Hop Wireless Ad-Hoc Network Routing Protocols in MANET", IJCSI International Journal of Computer Science Issues, 2011.
- [8] Abirami, K. Shanthi, "Sybil attack in Wireless Sensor Network", IJET, 2013.
- [9] S. Sharmila, G. Umamaheswari, "Detection of Sybil attack in Mobile Wireless Sensor networks", (IJESAT) International Journal of Engineering Science & Advanced Technology.