DETECTING SYBIL ATTACK USING HYBRID FUZZY K-MEANS ALGORITHM IN WSN

[1]Shipra Diwakar, [2]Dr. R. Kashyup
[1]Research Scholar, [2]HOD ECE
Rayat Bahara University Ropar, Punjab

ABSTRACT

Security in Wireless Sensor Networks is an important issue of concern in recent years. Many researchers have proposed various techniques for the detection and recovery of malicious nodes in the network and compared their merits and demerits with the existing approaches. Attacks in the network are caused due to the vulnerability of the nodes in the network, which results in the loss of data of the node and the routing data. In the proposed approach, a Hybrid Fuzzy K-means algorithm is used for the detection of Sybil attacks. The proposed approach combines the fuzzy approach and the k-means classification approach.

Keywords: Sybil Attack, WSN

1. INTRODUCTION

UWB transmission provides a security of the physical layer for wireless sensor network because of their huge bandwidth [1]. Certainly, wireless sensor network, which depend on the UWB radio signals, are essentially safer due to its low output power and short pulses of these signals. However, UWB signals can be snuffled by a strong-minded attacker, who is located nearer to the transmitter and it enable the latter to initiate an attack against the sensor network [2]. Thus, every class of wireless sensor network needed a strategy for security, which is implemented at each layer of the network protocol stack. Recently, the main focus is providing for security of wireless sensor network and the parameters on which main focus is given is routing, authentication, and key management, secure localization and secure aggregation [3]. Some secure ranging and localization protocols were particularly designed for preventing the integrity of ranging and for addressing location-related attacks in UWB WSNs. Signaling strategy are used to improve physical layer security of UWB systems. In last, a number of routing and clustering protocols attempt to address networking issues in UWB WSNs, lacking however advanced security features in their design [4].

Intrusion detection systems (IDSs) represent an significant in the arsenal of security experts against this type of attack [5]. Generally, IDS are categorized in two types:

1. Signature based intrusion detection systems.
2. Anomaly based intrusion detection systems.

According to latest researches, anomaly-based intrusion detection systems (ADSs) are well suited to wireless sensor network due to its flexibility and resource friendly behavior. Further, Anomaly-based techniques can be widely classified into prior-knowledge based andprior-knowledge free. In the framework of sensor network, rule-based detection appears to be very attractive, in the sense that the detection speed and complexity certainly benefits from the absence of an explicit training procedure [6]. A number of rule-based Sybil attack detection ADSs have been proposed so far that come with different analytical accuracy and varying degree of complexity. The fundamental detection mechanisms of these expert systems have based on an identity-based solution, a location verification approach or a visual-based method. While a number of anomaly detection algorithms exists in the literature, to the best of our knowledge, none of them is specifically designed for the emerging UWB transmission technology, the high precision ranging capability of which enables the ADS to not only detect, but also to localize the adversarial nodes by relying on internal tools, namely on accurate time-of-arrival (TOA)-based UWB distance measurements.

2. PROBLEM FORMULATION

Karapistoli, Eiriniet al [1] presenteda anomaly-based detection and location-attribution algorithm for cluster-based UWB WSNs. The presented approach defined a procedures for secure cluster formation, periodic re-clustering, and efficient cluster member monitoring.

Sarigiannidis, Panagiotiset al. [2] proposed a rule-based anomaly detection system. This proposed system helps to monitor and detect the Sybil attacks in wireless sensor network. This rule based system depends on the ultra-wideband (UWB) ranging-based detection algorithm which operates in a distributed. The result indicates that the proposed algorithm attains high detection accuracy and low false alarm rate.**Wang, Jiangtao, Geng Yang**et al. [3] a new method of Sybil attack detection in wireless sensor network (WSN) has been presented which is depending on received signal strength indication (RSSI). This process employed Jakes channel model by emulating real network space situation of sensor network. In this paper two ways are discussed to verify the raised efficiency and refinement of Sybil attack. The process attains the detection rate and provides several applications.

Lu, Aidong, Weichao Wanget al. [4] in this paper, a robust intrusion detection approach has been proposed for wireless sensor networks that is depending on a new multi-matrix visualization method with a set of pattern generation, evaluation, organization and interaction functions. The results indicate that the proposed detection approach can detect the Sybil attacks under distinct parameters. **Piro, Chris, Clay Shields**et al. [5] In this paper, detection mechanism has been proposed which indicates the mobility which may be enhance the security.

Particularly, the proposed scheme indicates that nodes can monitor traffic in the network and can locate a Sybil attacker that uses a number of network identities simultaneously. **Ghose, Sarbani**et al. [6]in this paper omnipresent wireless medium provides high mobility, yet the very nature of open medium introduces vulnerability. Earlier designs of security mechanisms concentrated more on the upper layers, but physical layer techniques have recently gained popularity. Security is taken care of by maximizing the information rate of the signal sent from the source to the receiver, with an assumption that the eavesdropper's channel is worse than the main channel. **Douceur, John R**et al. [7] in this paper, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. **Demirbas, Murat, and YoungwhanSong**et al. [8] proposed a robust and lightweight solution for sybil attack problem depending on received signal strength indicator (RSSI) readings of messages. The results of this proposed approach is robust as it locates all the sybil attacks. The performance indicates that the proposed approach is unreliable and time varying and radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome these problems.

3. PROPOSED METHODOLOGY

In order to solve the problem of security in wireless sensor networks, a hybrid approach is used. The hybrid approach is a combination of Fuzzy algorithm and the K- means classification algorithm. The fuzzy approach is used to create a relationship between the attributes and the labels (source node and targeted node) based on objective function. The K-means algorithm computes the mean value of the distance between the nodes and shifts the solution towards the calculated value. The combination of both the approaches helps in detecting the Sybil attack. The objective function used in the calculation can be computed as

$$ff = \sum w_1 . R_i + w_2 . E_j + w_3 . D_{i,j} \qquad (1)$$

Where R_i is the range of the source node

$E_j$are the residual energy of the target nodes and

$D_{i,j}$ is the distance between the source and the target node

The distance between the nodes is calculate using the Euclidian distance formula which is given by

$$D_{i,j} = \sqrt{((x_1 - x_2)\hat{}2 + (y_1 - y_2)\hat{}2\ )} \qquad (2)$$

Where $x_i and\ y_i$are coordinates of a node.

4. RESULTS AND DISCUSSIONS

To evaluate the performance of proposed approach following performance parameters are considered.

End-to-End Delay: it is given by:

$$Delay = (packet\ received\ by\ receiver\ time - generated\ time)$$

Figure 1 shows the comparison between the SimBet function and the proposed trust approach with respect to time. The delay in the proposed approach reduces because of the reduction in number of retransmissions.

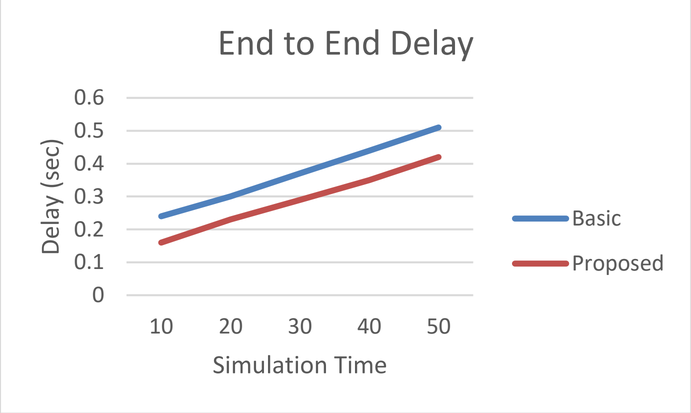

Fig 1: Packet Delivery Delay

Packet Delivery Ratio

It is defined as follows:

$$\text{Packet Delivery Ratio} = \frac{\text{Total Receievd Packets}}{\text{Total Generated Packets}}$$

Packet loss due to collision is reduced largely by allocating timeslots. Now the packet loss occurs due to failure of links in mobile environment. Figure 2 shows the graph between packet delivery ratio and the simulation time.

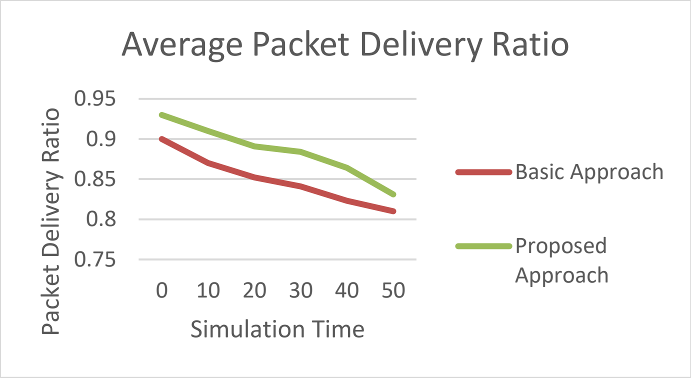

Fig 2 Packet Delivery ratio

Throughput

It is the rate of successful message delivery over a communication channel.

$$\text{Throughput} = \frac{\text{Packet Size} * \text{Number of Packets Delivered}}{\text{Total duration of Simulation}}$$

Figure 3 shows the graph of the throughput plotted against the simulation time.

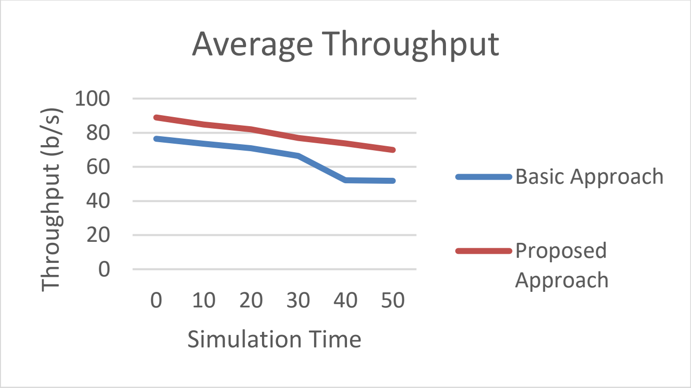

Fig 3 Throughput of the network

CONCLUSION

Security related application in Wireless Network are the major area of concern in recent years. Many approaches have been proposed for various types of attacks in the network. In the proposed approach a hybrid of Fuzzy and K-means classification is proposed which detects and works against the Sybil attacks. The proposed methodology is implemented using NS2 and the results shows that the proposed approach outperforms the basic approach by a significant value. The comparison parameters are end to end delay, packet delivery ratio and the throughput of the network and the approaches are compared against the simulation time. In future other machine learning approaches must be proposed and compared with the existing approaches.

REFERENCES

[1] Karapistoli, Eirini, and Anastasios A. Economides. "ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks." *EURASIP Journal on Information Security* 2014, no. 1 (2014): 1-12.

[2] Sarigiannidis, Panagiotis, EiriniKarapistoli, and Anastasios A. Economides. "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information." *Expert Systems with Applications* 42, no. 21 (2015): 7560-7572.

[3] Wang, Jiangtao, Geng Yang, Yuan Sun, and Shengshou Chen. "Sybil attack detection based on RSSI for wireless sensor network." In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pp. 2684-2687. IEEE, 2007.

[4] Lu, Aidong, Weichao Wang, Abhishek Dnyate, and Xianlin Hu. "Sybil attack detection through global topology pattern visualization." *Information visualization* 10, no. 1 (2011): 32-46.

[5] Piro, Chris, Clay Shields, and Brian Neil Levine. "Detecting the sybil attack in mobile ad hoc networks." In *Securecomm and Workshops, 2006*, pp. 1-11. IEEE, 2006.

[6] Ghose, Sarbani, and Ranjan Bose. "Physical layer security in UWB networks." In *Microwaves, Communications, Antennas and Electronics Systems (COMCAS), 2011 IEEE International Conference on*, pp. 1-5. IEEE, 2011.

[7] Douceur, John R. "The sybil attack." In *Peer-to-peer Systems*, pp. 251-260. Springer Berlin Heidelberg, 2002.

[8] Demirbas, Murat, and Youngwhan Song. "An RSSI-based scheme for sybil attack detection in wireless sensor networks." In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pp. 564-570. IEEE Computer Society, 2006.