Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 02 Issue 02 - 2021 (July to December)

Page 12:16

Malicious Node Detection in Adhoc Wireless Sensor Networks Using Secure Trust Protocol

Dr.Pravin R. Kshirsagar
Computer Science & Communication Engineering;Bio-Engineering and Technology
G.H. Raisoni College of Engineering, Nagpur
ORCHID ID-0000-0002-7381-6284
pravinrk88@yahoo.com

Article History

Received: 15 July 2021
Revised: 20 September 2021
Accepted: 22 November 2021

Abstract

Recent researches in different perspectives and industrialized oriented applications have broadly utilized wireless Sensor Network (WSN). At present, WSN have attained specialist attention for providing secure networks, which is free from attackers and malicious nodes. WSN security is subject to threats by assaulters. It needs sensor to periodically sense and transmit sensitive data to BS for data transmitting commonly through multi hop path. As, it is very essential to design the secure AdHoc network to detect the smart attackers efficiently. Here in this paper we design trust based secure network for detection of attacks due to presence of malicious nodesutilizing secure trust protocol (STP) scheme of AdHoc wireless sensor network. Clustered Heterogeneous Routing Protocol (CHRP) has been used to improve network security. Using factors including throughput, minimal end-to-end delay, packet transmission rate, energy conservation rate, and attack detection rate, experimental results demonstrate better network security.

Keywords: malicious nodes, Adhoc network, STP, CHRP,throughput, minimized end-end delay, packet delivery rate.

1. INTRODUCTION

In order to collect, aggregate, and analyse data, WSN typically comprises of a large number of sparse sensor nodes (SNs) placed throughout an operational region. A WSN is susceptible to numerous attacks because of its exposure to outdoor conditions and the inherent unreliability of wireless communication [1].It is a recent development in network technologies and has been growing progressively [2]. WSNs have a significant scientific and societal impact. Insider attacks and outsider assaults are two categories for malicious attacks on WSNs.Insider assaults are far more difficult to handle, even though most external attempts, such as replay, spoofing, and Sybil attacks, can be stopped by authentication and cryptography [3]. Data packets in a WSN based on a BS must be forwarded to BS utilising multi-hop routing and SNs acting as relays [4]. Since compromised SNs nearby can most effectively intercept data packets transmitted to BS to interfere with basic data delivery capabilities, SNs adjacent to BS are suitable targets for capture attacks.

2. LITERATURE SURVEY

Energy and security, which have been explored from various angles, have been regarded the two key challenges by WSN. Work in [5] gives a straightforward and effective implementation of Lloyd's k-means clustering algorithm, which they refer to as the filtering algorithm, as have other related studies that have been detailed below. For dependable and effective data acquisition in a stationary WSN with transfaulty nodes, the author in [6] recommends the ReDASTsystem.For the purpose of understanding dynamics between adversary activity as well as protection for cyber physical systems, author [7]. A fair trust-based malicious node detection and isolation (FTMNDI) scheme's performance is examined in work in [8].A unified framework is proposed in [9] design and build a system employing the process described above, in which low-level attack detection is carried out in sensors with simple rules as well as high-level attack detection is carried out in sinks as well as at BS with complicated rules. For secure position estimate of SNs appropriate for security-sensitive WSN applications, author [10] proposes a novel security architecture.

3. SYSTEM MODEL:

This section discusses the architecture of a trust-based secure network for detection of attacks caused by existence of malicious nodes in an ad hoc WSN using secure trust protocol (STP) system. Additionally, it makes use of clustered heterogeneous routing protocol (CHRP), which can significantly improve network security.The quantity of effective events and the stored events received on the CH are used by the base station to perform various operations. The base station eliminates redundant events and those that were brought on by a network issue rather than outsiders:

*Ei*D [*Ty*; *t*; *Attack_ID*; *Source_ID*; *Dest_D*]

Below is a flow diagram of suggested system.

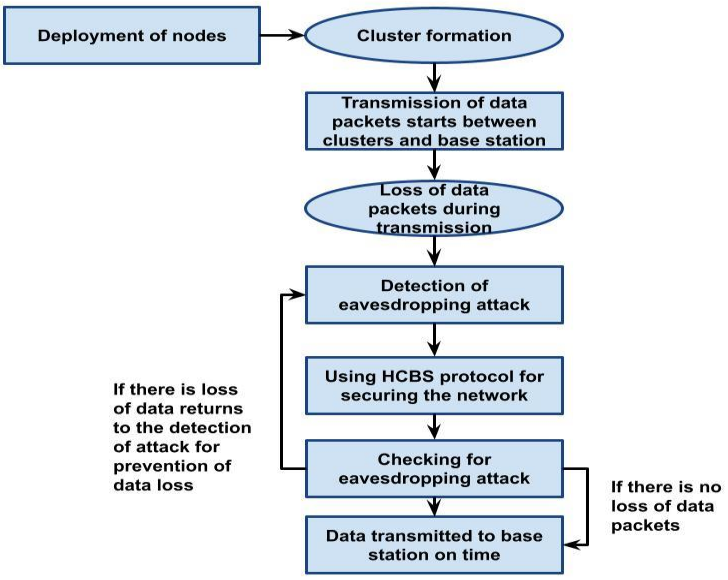

Fig-1 Block Diagram for TSDAMN

Assume that x is the maximum number of retransmissions needed for data packets to arrive at their destination successfully. Every time a transmission attempt is made, the source node randomly selects a back-of time from the range [Cmin, CWc y], where CWc y stands for the size of the contention window of node c during that particular transmission attempt and is determined as follows using the exponential back-of algorithm:

$$ETX = \frac{d_{i,j}}{\left(1 - \prod_{>i}\left(1 - \mu_i(t_n)\lambda_c(t_n)\right)\right)\left(1 - \prod_{j>c}\left(1 - \mu_c(t_n)\lambda_d(t_n)\right)\right)}\frac{S}{B}, t \in [t_n, t_{n+1}]$$

The multi-path mp model is employed the distance is greater than or equal to threshold value, which is indicated by d0. whereas (2) provides energy consumption for node j's receiving a packet of bits of data:

$$E_t(i,j) = \begin{cases}\left(\delta_t + \theta_{fs} D^2_{(i\leftrightarrow j)}\right)\beta, & D_{(i\leftrightarrow j)} < d_0 \\ \left(\delta_t + \theta_{mp} D^4_{(i\leftrightarrow j)}\right)\beta, & \text{otherwise}\end{cases}$$

where$d_0 = \sqrt{\theta_{fs}/\theta_{mp}}$

$$E_r(j) = \delta_r \beta$$

Figure 1 shows the network design that was used in this study. We presume that every node between d and d + r is a part of stage j of the network described in (3), or in a future stage, subject to node position restrictions and transmission area R's boundaries.

$$N_i^{\text{localization}} \in \left[d_j, d_j + r\right] \overset{\text{stage}}{\Leftrightarrow} N_{i,j}, j \in [2, N]$$

$$Tv_{N_{k,l}}^{N_{i,j}} = NC^{(LO_{k,l}-1)} + \sum_{m\in[j,j+1], n\in[[1,2]|k\}} \left(EC_{k,l}^{LO_{k,l}} - \frac{EC_{m,n}^{Lo_{m,n}}}{w}\right) + SN_{i,j} * SN_{k,l}^{LO}$$

The trust value strikes a balance between three key factors. The first is the number of active connections, which favours nodes in next stage over those in the one they are currently in. The second is the residual energy EC, which is difference between candidate node's energy and sum of all the other energy nodes. The third is state node SN, which is created based on the node couples' states. We observe that various components of Tv formula are directly impacted by candidate node's location (4). Trust value, which defines path from SN to sink node, is therefore greatly influenced by node's location.

4. PERFORMANCE ANALYSIS

The experimental findings include metrics such as packet drop calculation, PDR, energy efficiency calculation, energy consumption calculation, and end-to-end latency for proposed TSDAMN under black hole and worm hole attacks.

Parameters	ReDAST	FTMNDI	MND_WSN_STP
Packet drop calculation	45	43	41
PDR	91	93	95
Energy efficiency calculation	88	91	94
Energy consumption calculation	55	56	58
End-End delay	41	43	45

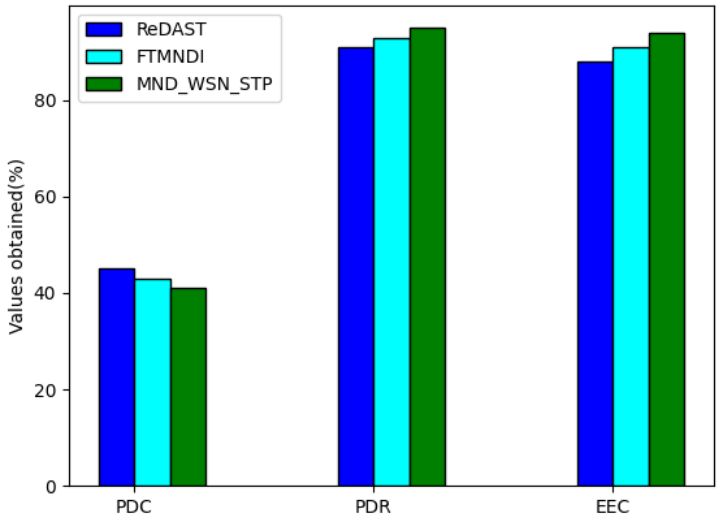

Figure 2: Comparison

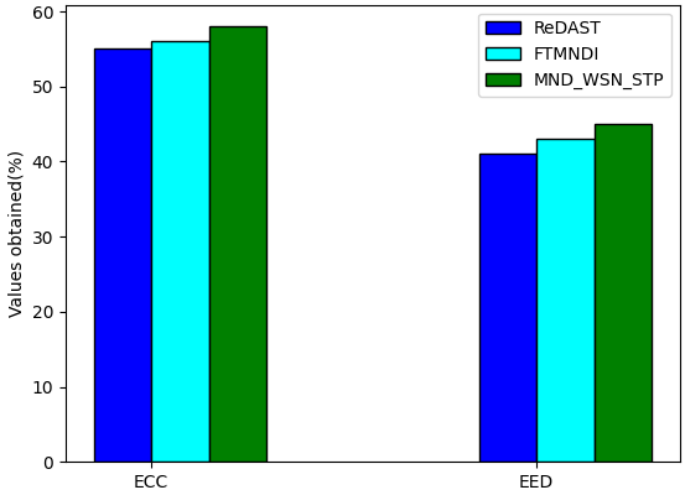

Figure 3: Comparison of proposed with existing

Performance analysis therefore displays attack detection rate in terms of packet loss, PDR, energy effectiveness, energy consumption, and end-to-end delay. Additionally, characteristics of energy consumption, packet loss, PDR, throughput, and end-to-end delay have been used to compare the existing system to the proposed system.

5. CONCLUSION

Therefore, we created a trust-based secure network for the AdHoc wireless sensor network to identify attacks caused by presence of malicious nodes (TSDAMN). Heterogeneous Cluster Based Secure (HCBS) routing technology isutilized to improve network security.In comparison to the existing FTMNDI and the proposed TSDAMN, the experimental results demonstrate improved network security in terms of throughput, minimized end-to-end delay, packet transmission rate, energy conservation rate, attack detection rate.

REFERENCES

[1] She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access*, *7*, 38947-38956.

[2] Qiuwei Yang,1Xiaogang Zhu,2 Hongjuan Fu,1 and XiqiangChe , "Survey of Security Technologies on Wireless Sensor Networks", Volume 2015, Article ID 842392.

[3] Jaint, B., Singh, V., Tanwar, L. K., Indu, S., &Pandey, N. (2018, October). An efficient weighted trust method for malicious node detection in clustered wireless sensor networks. In *2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)* (pp. 1183-1187). IEEE.

[4] FirasZawaideh, MuhammedSalamah Hussein Al-Bahadili, "A Fair Trust-Based Malicious Node Detection and Isolation Scheme for WSNs", *IT-DREPS Conference, Amman, Jordan Dec 6-8, 2017.*

[5] Kumar, S., &Mehfuz, S. (2019, March). A PSO based malicious node detection and energy efficient clustering in wireless sensor network. In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 859-863). IEEE.

[6] Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. *IEEE Transactions on Reliability*, *69*(3), 1077-1086.

[7] Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., & Thong, P. H. (2019). Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. *Computer Standards & Interfaces*, *66*, 103358.

[8] Smys, S., & Raj, J. S. (2019). Performance optimization of wireless adhoc networks with authentication. *Journal of Ubiquitous Computing and Communication Technologies (UCCT)*, *1*(02), 64-75.

[9] Zawaideh, F., &Salamah, M. (2019). An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *International Journal of Communication Systems*, *32*(3), e3878.

[10] Anwar, R. W., Zainal, A., Outay, F., Yasar, A., &Iqbal, S. (2019). BTEM: Belief based trust evaluation mechanism for wireless sensor networks. *Future generation computer systems*, *96*, 605-616.