Research Article

Trust-Based Secure Network For Detection Of Attacks (Wormhole And Black Hole) Due To Malicious Nodes In Ad Hoc Wireless Sensor Network

Ashok Babu.Chatla[1], B.Maji[2], Habibulla Khan[3], B T P Madhav[4]

[1]Department of Electronics and Communication Engineering National Institute of Technology, Durgapur, India
[2]Department of Electronics and Communication Engineering National Institute of Technology, Durgapur, India
[3]Dept of Electronics and Communication Engineering K L University, Vaddeswaram, Guntur, AP, India
[4]Dept of Electronics and Communication Engineering Koneru Lakshmaiah Education Foundation Vaddeswaram, Guntur, AP, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

ABSTRACT

Recent researches about in alternate points of view and industrialized situated applications have comprehensively used Wireless Sensor Network (WSN). At present, WSN have achieved the authority consideration for giving the protected systems, which is free from the assailants and vindictive hubs. The remote sensor systems security can be liable to dangers by assaulters. It requires the sensor to sporadically detect and transmit touchy information to the base station for information transmitting generally through multi bounce way. As, it is exceptionally fundamental to plan the safe Ad Hoc system to identify the savvy assailants productively. Here in this paper we configuration trust based secure system for discovery of assaults (wormhole and dark opening) because of the nearness of noxious hubs (TSDAMN) plan of Ad Hoc remote sensor organize. For the upgrade of system security Heterogeneous Cluster Based Secure (HCBS) directing convention has been utilized. The test results indicates security enhanced system with the parameters like throughput, limited end-end delay, parcel transmission rate, vitality preservation rate, assault discovery rate.

Keywords: Malicious nodes, Adhoc network, TSDMN, HCBS, throughput, minimized end-end delay, packet delivery rate.

INTRODUCTION

A wireless sensor network (WSN) for the most part comprises of an expansive number of modest sensor nodes (SNs) sent in an operational territory for information detecting, amassing, and preparing. The introduction to regular habitats and the innate shakiness of wireless transmission make a WSN powerless against numerous assaults [1]. Wireless sensor networks, as a developing network innovation, have risen bit by bit as of late. They can acquire a ton of point by point and dependable data in the network conveyed region whenever and anyplace; in this way, they are generally utilized in military barrier, industry, horticulture, development and urban administration, biomedical and natural observing, fiasco help, open wellbeing and antiterrorism, perilous and unsafe territorial remote control, et cetera which are abundantly accounted by numerous legislatures. Wireless sensor networks have a vital logical and down to earth esteem.

SNs sent in antagonistic conditions for military applications likewise could be endangered through catches and end up vindictive. In addition, because of extreme asset requirements of SNs, for example, vitality, memory, and computational power, customary vitality devouring protection instruments like open key foundation and host-based interruption location systems may not be possible. The quick advancements in wireless correspondence, sensor innovation, and implanted processing innovation have advanced the rise and improvement of wireless sensor networks (WSN).

Wireless sensor networks comprise of a substantial number of shoddy miniaturized scale sensor nodes sent in the checking region, which is a multihop self-sorting out network framework shaped by wireless specialized technique, whose reason for existing is to detect, gather, and process agreeably the data detected by sensors in the network disseminated zone and after that forward the outcomes to its users.[2]

Pernicious assaults to WSNs can be characterized into untouchable assaults and insider assaults. While most untouchable assaults, for example, mocking, replay and Sybil assaults can be forestalled by validation and cryptography, insider assaults are considerably harder to manage. In this paper, we build up a trust-based interruption recognition framework (IDS) plot using an exceptionally adaptable progressive trust administration convention for grouped wireless sensor networks to recognize inside aggressors. In a base station based wireless sensor network (WSN), information parcels must be sent to the base station (BS) by means of multi-jump steering utilizing sensor nodes (SNs) as transfers. SNs near the BS (called basic SNs) are alluring focuses for catch assault since traded off SNs near the BS can best block information parcels sent to the BS to disturb the essential information conveyance usefulness. In the writing, different plans have been intended for safeguarding basic SNs from vitality fatigue in order to drag out the framework lifetime; in any case, how to counter specific catch, i.e., basic SNs are tar-gets of particular catch assaults, is an open issue [1]. Once a hub is caught and transformed into a malignant hub, it turns into an inside assailant. Demonstrating shrewd assailant practices and concentrate their consequences for security is little investigated in the writing and is another open issue. [3]

Characteristics of WSN

- Power consumption constraints for nodes using batteries or energy harvesting

- Ability to cope with node failure (resilience)
- Mobility of nodes.
- Heterogeneity of nodes.
- Scalability to large scale of deployment
- Ability to withstand harsh environment conditions.

LITERATURE SURVEY

WSN has considered the principle issues as vitality and security which have been examined in various angles. The related works has been talked about underneath,

Tapas Kanungo, Senior Member, IEEE, David M. Mount, Member, IEEE, Nathan S. Netanyahu,2002 presents a basic and effective execution of Lloyd's k-implies bunching calculation, which we call the separating calculation. This calculation is anything but difficult to actualize, requiring a kd-tree as the main real information structure. They set up the viable effectiveness of the separating calculation in two different ways.

Right off the bat, present an information touchy investigation of the calculation's running time, which demonstrates that the calculation runs quicker as the detachment between bunches increments. Besides, present various observational investigations both on artificially produced information and on genuine informational collections from applications in shading quantization, information pressure, and picture division. [4]

Pushpendu Kar, Student Member, IEEE and Sudip Misra, Senior Member, IEEE, 2016 proposes a plan, named ReDAST, for dependable and productive information procurement in a stationary WSN within the sight of transfaulty nodes. Due to the transfaulty conduct, a sensor hub gets incidentally segregated from the network. Brief hub separation prompts the arrangement of dynamic correspondence gaps in the network, which shape and vanish progressively. Further, they may increment or abatement in measure powerfully too. These impacts result in loss of data in the radiation influenced territory. To forestall data misfortune in WSN due to transfaulty conduct of sensor nodes, in the proposed conspire, we develop the network utilizing sensor nodes having double method of correspondence – RF and acoustic. To get excess inclusion inside a radiation influenced region, all the sensor nodes in the zone wind up enacted and change to the acoustic correspondence mode subsequent to identifying themselves to be influenced by radiations. In-network information combination is performed to get genuine data from the excess data got from the radiation-influenced region. [5]

Robert Mitchell and Ing-Ray Chen, Member, IEEE, 2015 build up an explanatory model in view of stochastic Petri nets to catch the elements between foe conduct and protection for digital physical frameworks. We consider a few kinds of disappointments including wearing down disappointment, invasion disappointment, and exfiltration disappointment which can happen to a digital physical framework. Utilizing a modernized electrical matrix for instance, we outline the parameterization procedure. [6]

Firas Zawaideh, Muhammed Salamah, Hussein Al-Bahadili, 2017 explores the exhibitions of a reasonable trust-based pernicious hub location and disengagement (FTMNDI) plot. This plan utilizes an altered adaptation of the neighbor-weight trust assurance (NWTD) calculation to occasionally refresh the trust of the nodes in light of their notoriety.

At that point, a hub inside the network is confined if its trust turns out to be not exactly a pre-set least satisfactory trust esteem. [7]

Jun Wu, Kaoru Ota, Mianxiong Dong, And Chunxiao Li, 2015 outline and actualize a framework utilizing the component depicted over, a unified structure is proposed in which low-level assault recognition with straightforward principles is performed in sensors, and abnormal state assault identification with complex guidelines is performed in sinks and at the base station. Besides, programming characterized networking and network work virtualization advances are utilized to perform assault moderation when either low-level or abnormal state assaults are recognized. [8]

Sana H. Jokhio1, Imran Ali Jokhio2, Andrew H. Kemp3, 2013 propose a novel security system for secure area estimation of sensor nodes appropriate for security-touchy WSN applications. The proposed structure means to give security, versatility, flexibility and streamline control utilization amid the protected area estimation period of a wireless sensor network. The outlined structure comprises of a two-way validation conspire, a light-weight encryption system and a novel secure key age calculation. The investigation examines qualities of the segments whenever utilized for secure confinement exclusively and in addition when utilized together as intelligent parts of a security system for WSN applications. [9]

S.H. Jokhio1 I.A. Jokhio2 A.H. Kemp3, 2011 proposes the novel sensor hub catch assault recognition and safeguard (SCADD) convention. SCADD gives a financially savvy arrangement against the hub trade off and catch assaults in WSNs, improving the general WSN security for security-touchy applications. This convention comprises of two building squares: hub assault identification square and resistance supporting measure square. The previous gives vital based assault location to dispense with the likelihood of misconception and the last uses an implosion barrier measure against hub catch assault, without really wrecking the hub's radio administration, to stay away from a noteworthy security break. [10]

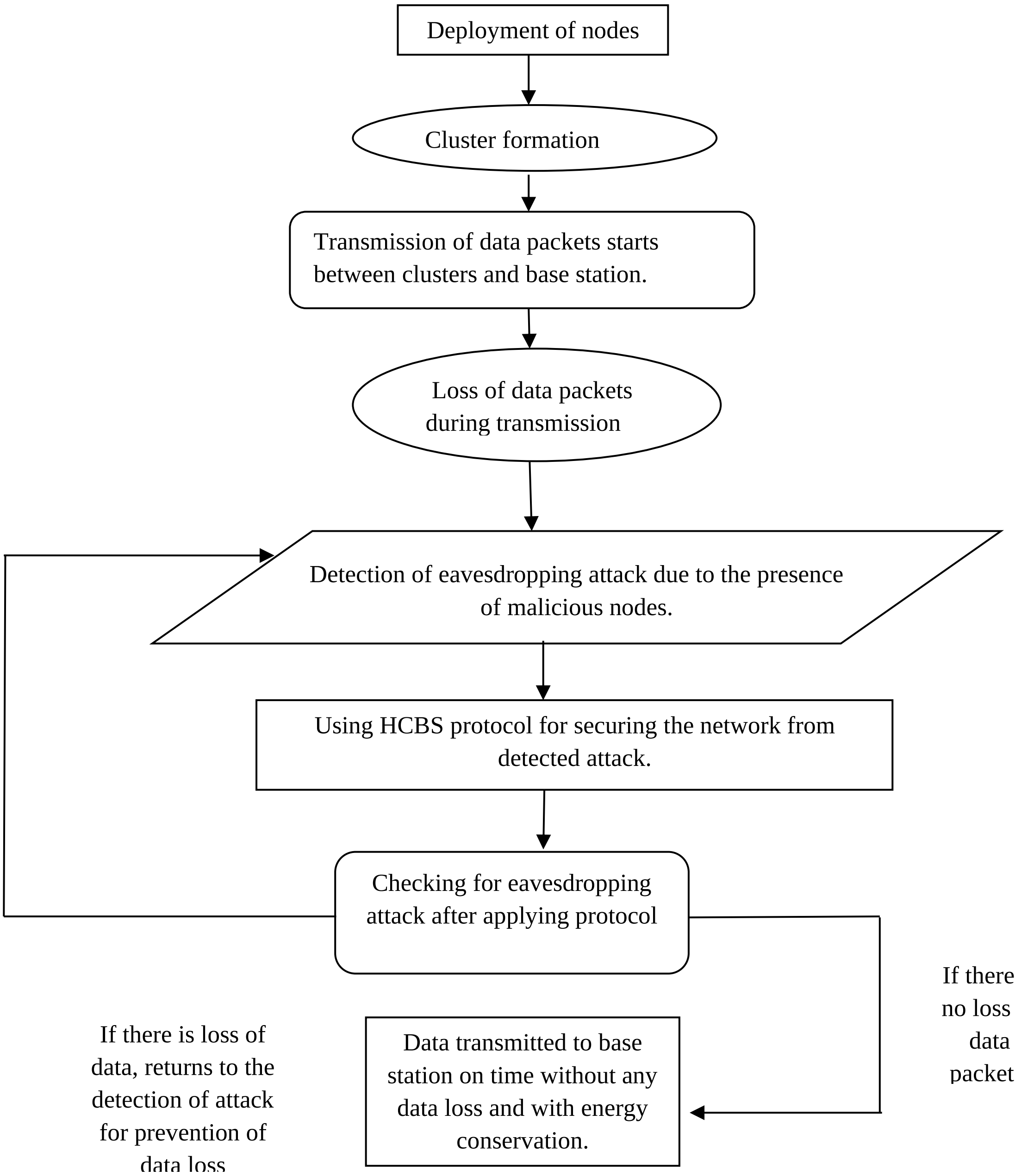
Boyuan Sun And Donghui Li, 2018 proposed trust demonstrate depends on an enhanced sliding time window considering assault recurrence to encourage the revelation of malignant practices of assailants. Joined with successful steering location and upkeep convention, the execution of our answer is tried through a wide arrangement of recreation tests. [11]

RESEARCH METHODOLOGY:

Since the security related concerns are the real issues of WSN, the productive network must be free from the malignant nodes and from every one of the dangers and assaulters. So in this paper we talk about the outline trust based secure network for location of assaults (wormhole and dark gap) because of the nearness of vindictive nodes (TSDAMN) plan of AdHoc wireless sensor network.

It likewise utilizes the convention for anchoring the network called Heterogeneous Cluster Based Secure directing convention (HCBS) which can contribute for the most part on the upgrade.

The flow diagram of the proposed system is given below


Deployment of nodes
Cluster formation
Transmission of data packets starts between clusters and base station.
Loss of data packets during transmission
Detection of eavesdropping attack due to the presence of malicious nodes.
Using HCBS protocol for securing the network from detected attack.
Checking for eavesdropping attack after applying protocol
If there is loss of data, returns to the detection of attack for prevention of data loss
Data transmitted to base station on time without any data loss and with energy conservation.
If there is no loss of data packets.

The proposed plot has been contrasted and the exhibitions of a reasonable trust-based pernicious hub identification and disconnection (FTMNDI) conspire [7].

In FTMNDI, all sensor nodes are at first accepted completely trusted with their trust esteem set to 1. At that point, if the checking hub sees one of the nodes transmitting misrepresented data (i.e. a hub is carrying on vindictively), it distinguishes it as a genuine positive noxious hub. At that point any malignant hub inside the network is secluded if its trust turns out to be not exactly a pre-set MAT. The execution of the FTMNDI plot is assessed through various reenactments utilizing the network test system MANSim.

These reproductions research the impact of number of checking nodes, trust refresh factor and least worthy trust on the noxious hub lifetime. Utilizing information envelopment investigation, we additionally found the most prevailing component and the close ideal estimations of the above parameters. The construct station performs different capacities with respect to the put away occasions got on the CH and the quantity of powerful occasions. Repetitive occasions and those that were caused by some network condition and not by interlopers are dispensed with by the base station:

$$Ei \text{ D } [Ty; t; Attack\_ID; Source\_ID; Dest\_D]$$

PERFORMANCE ANALYSIS

The experimental results the parameters at case of black hole attack and worm hole attack for proposed TSDAMN like packet drop calculation, packet delivery rate, energy efficiency calculation, energy consumption calculation, end-to-end delay.

- **Packet drop calculation:**

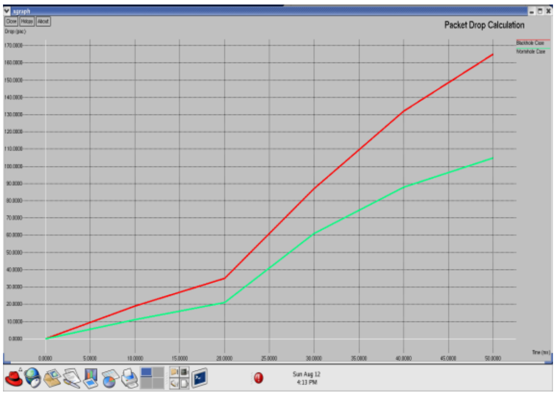


Fig-2 packet drop calculation

Figure-2 shows the packet drop calculation at presence of black hole attack and worm hole attack.

- **Packet delivery rate:**

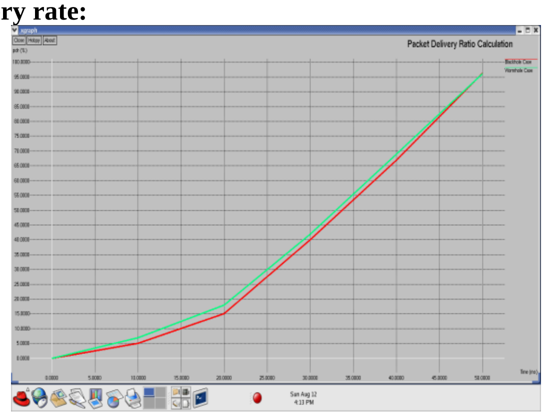


Fig-3 packet delivery calculation

Figure-3 shows the packet delivery calculation at presence of black hole attack and worm hole attack.

- **Energy efficiency calculation:**

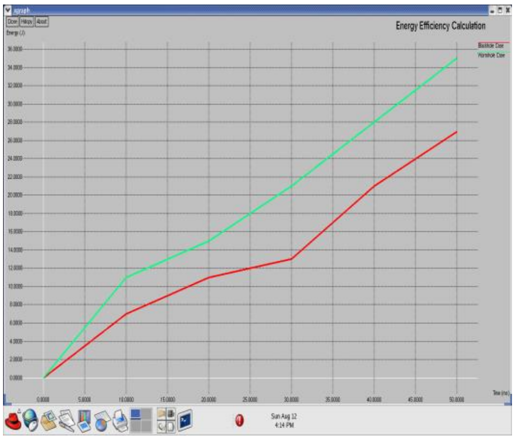


Fig-4 energy efficiency calculation

Figure-4 shows the energy efficiency calculation at presence of black hole attack and worm hole attack.

- **Energy consumption calculation:**

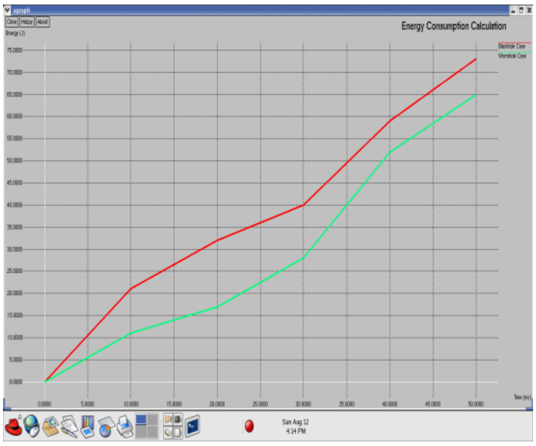


Fig-5 energy consumption calculation

Figure-5 shows the energy consumption calculation at presence of black hole attack and worm hole attack.

- **End-to-end delay:**

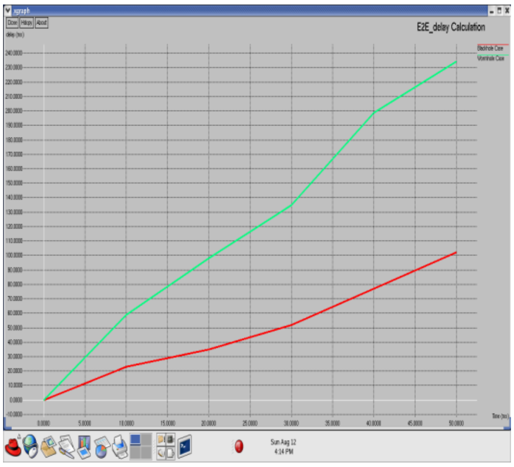


Fig-6 end to end delay calculation

Figure-6 shows the end to end calculation at presence of black hole attack and worm hole attack.

COMPARISON RESULTS BETWEEN TSDAMN AND FTMNDI

- **Energy consumption:**

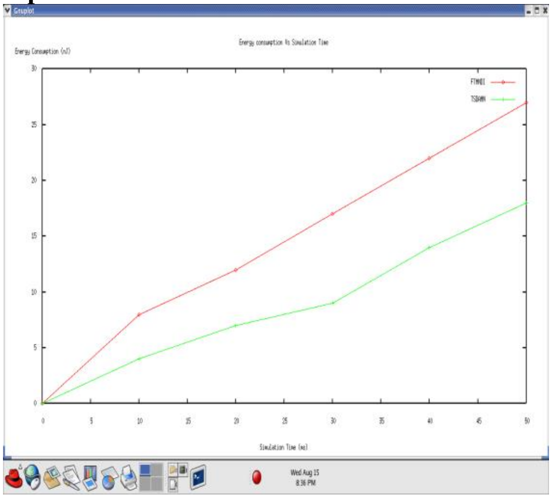


Fig-7 energy consumption

Fig-7 shows the energy consumption comparison between the proposed TSDAMN and existing FTMNDI.

- **Packet loss:**

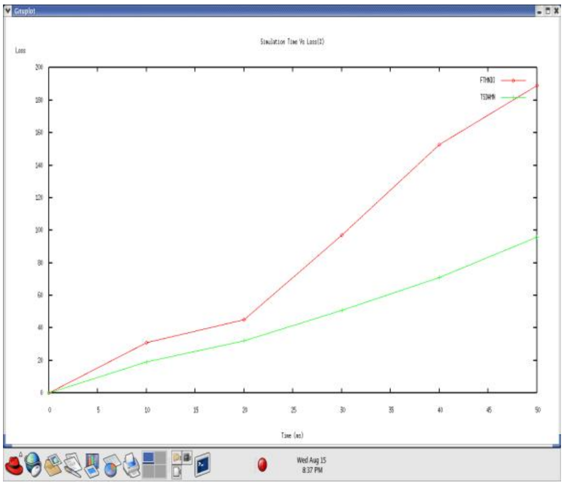


Fig-8 packet loss

Fig-8 shows the packet loss ratio between proposed TSDAMN and existing FTMNDI.

- **Packet delivery ratio:**

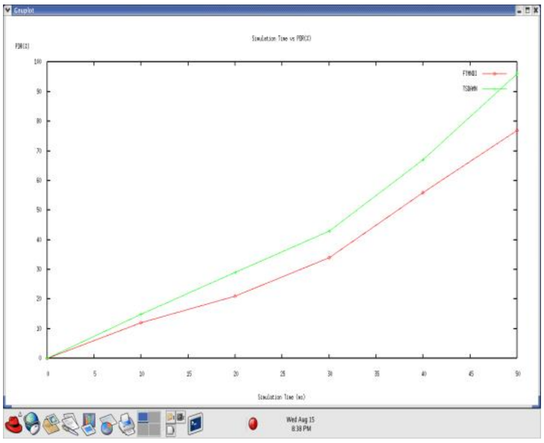


Fig-9 packet delivery ratio

Fig-9 shows the packet delivery ratio between proposed TSDAMN and existing FTMNDI.

- **Throughput**

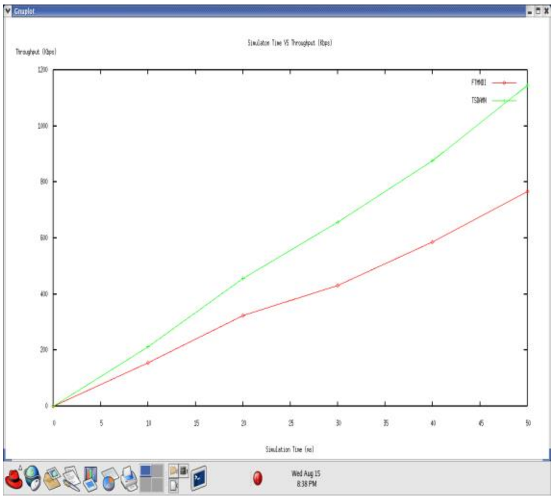


Fig-10 throughput

Figure-10 shows the throughput comparison between proposed TSDAMN and existing FTMNDI.

- **End-to- end delay:**

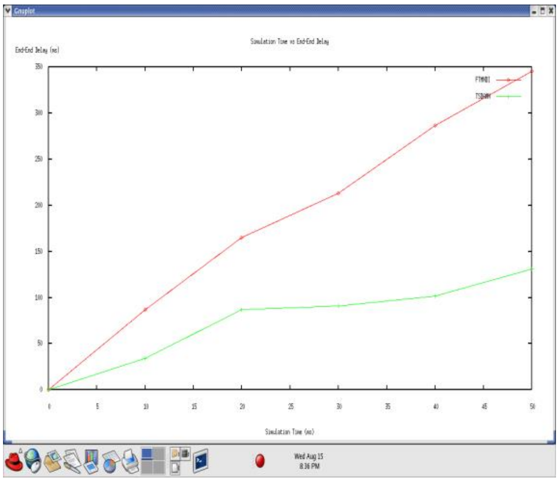


Fig-11 end to end delay

Figure- 11 shows the end to end delay between proposed TSDAMN and existing FTMNDI.

Hence the performance analysis shows the attack detection rate in terms of packet drop, packet delivery, energy efficiency, energy consumption, and end to end delay. And also the existing system has been compared with the proposed system with the parameters of energy consumption, packet loss, packet delivery ratio, throughput and end to end delay.

CONCLUSION

Subsequently we outlined trust based secure network for discovery of assaults (wormhole and dark gap) because of the nearness of malignant nodes (TSDAMN) plan of AdHoc wireless sensor network. For the improvement of network security Heterogeneous Cluster Based Secure (HCBS) directing convention has been utilized. The exploratory outcomes indicates security enhanced network with the parameters like throughput, limited end-end delay, bundle transmission rate, vitality protection rate that has been contrasted and existing FTMNDI and the proposed TSDAMN, assault identification rate regarding parcel misfortune, parcel conveyance, vitality proficiency, vitality utilization and end to end delay.

REFERENCES

1. Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Cho, “Trust-Based Intrusion Detection in Wireless Sensor Networks”, IEEE ICC 2011.
2. Qiuwei Yang,1 Xiaogang Zhu,2 Hongjuan Fu,1 and Xiqiang Che , “Survey of Security Technologies on Wireless Sensor Networks”, Volume 2015, Article ID 842392.
3. Hamid Al-Hamadi and Ing-Ray Chen, *Member, IEEE*, “Adaptive Network Defense Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks”, DOI 10.1109/TNSM.2015.2441059, IEEE Transactions on Network and Science Management.
4. Tapas Kanungo, Senior Member, IEEE, David M. Mount, Member, IEEE, Nathan S. Netanyahu, Member, IEEE, Christine D. Piatko, Ruth Silverman, and Angela Y. Wu, Senior Member, IEEE, “An Efficient k-Means Clustering Algorithm: Analysis and Implementation”, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 24, NO. 7, JULY 2002.
5. Pushpendu Kar, Student Member, IEEE and Sudip Misra, Senior Member, IEEE, “Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes”, DOI 10.1109/TNSM.2016.2516243, IEEE Transactions on Network and Service Management.
6. Robert Mitchell and Ing-Ray Chen, *Member, IEEE*, “Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber Physical Systems”, 0018-9529 © 2015 IEEE.
7. Firas Zawaideh, Muhammed Salamah Hussein Al-Bahadili, “A Fair Trust-Based Malicious Node Detection and Isolation Scheme for WSNs”, *IT-DREPS Conference, Amman, Jordan Dec 6-8, 2017.*
8. JUN WU1, (Member, IEEE), KAORU OTA2, MIANXIONG DONG2, AND CHUNXIAO LI, “A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities”, Digital Object Identifier 10.1109/ACCESS.2016.2517321.
9. Sana H. Jokhio1, Imran Ali Jokhio2, Andrew H. Kemp, “Light-weight framework for security-sensitive wireless sensor networks applications”, IET Wirel. Sens. Syst., 2013, Vol. 3, Iss. 4, pp. 298–306 doi: 10.1049/iet-wss.2012.0127.
10. S.H. Jokhio1 I.A. Jokhio2 A.H. Kemp, “Node capture attack detection and defence in wireless sensor networks”, IET Wirel. Sens. Syst., 2012, Vol. 2, Iss. 3, pp. 161–169 161 doi: 10.1049/iet-wss.2011.0064.
11. BOYUAN SUN AND DONGHUI LI, “A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs”, *Digital Object Identifier 10.1109/ACCESS.2017.2786944*.