ISSN 2278-3091
Volume 10, No.1, January - February 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse071012021.pdf
https://doi.org/10.30534/ijatcse/2021/071012021

HTBIDS: Hybrid Trust Based Intrusion Detection System for Physical Layer in WSN

Bikash RanjanBag[1], Umashankar Ghugar[2]
[1,2]Department of Computer Science
Berhampur University,Berhampur-760007, India
bikashbag@gmail.com, umaghugar@gmail.com

ABSTRACT
In recent years, wireless sensor network (WSN) is the measure concern over network communication. A number of attacks are occurred at the time of network communication as result it hampers the smooth functionality, data flow and data transmission. In this article, we have proposed a trust-based intrusion detection system for physical layers attacks using DRI and Cross Check method. The HTBIDS is effective method to identify the abnormal nodes in wireless sensor network. The abnormal nodes are attacked by periodic jamming attack. We have considered the periodic jamming attack at physical layer for performance evaluation. Results show that HTBIDS performs better using detection accuracy (DA) and false alarm rate (FAR).

Keywords: Trust, Cluster head (CH), Senso rnode (SN),Intrusion Detection System (IDS)

1. INTRODUCTION

Wireless sensor network (WSN) has led to the top priority among the network communication. Its applications are used in different areas such as satellite communication, industry, signal transmitted under water, medical sector, defense surveillance, home affirmation, and banking transaction etc. It is a scattered network and contain sensor nodes deployed in a special environment. This sensor node is used as a Teenage computing system with minimal calculating tools [1], [2]. It senses the natural conditions like heat, humidity, sound, compression, and wave at several areas [3], [4]. The security in WSN is an unsolved issue from the last few years. Here a number of attackers hamper the network communication through different inside and outside attacks. The intruder can jam the communication process through radio frequencies [5]. The IDS sense the intruder such that the computer displays a behavior of the node against another node and implements an intruder solution [6]for the of smooth functionality of nodes and data communication over the networks.IDS is a crucial component of WSNs. It is used to detect the unauthorized access and monitors the activity of the nodes in the network. It is always ready to defend against an attacker or malicious node [7]. Recently, researchers have proposed several models based on IDS that uses trust management, game theory, immune theory, data mining, machine learning and statistical model [8]. Trust based system is one of the most impressive method. From the last few years, number of researchers have presented their models on IDS using trust-based system.

The suggested method in this paper is to detect the attacker, where intrusion is identified using the trust metrics principle of physical layer protocol using deviation factor. The highlights include:

1.HTBIDS is suitable for identification of periodic jamming attack at physical layer.

2.This method is based on AODV routing protocol. We use the proposed algorithm when data packet transmission starts. It is based on two methods i.e.

a) We use trust metrics to measure the trust value of each node. In this process, the monitoring node measures the main factor of the physical layer of the node being monitored and then computes individual trust values. The trust value is then conveyed periodically to the top of the CH. CH determines whether the SN is a valid or anomalous node using a trust test.

b) After getting the trust sensor node, we transmit the trust-sensor-node through the DRI and cross-checking mechanism to the destination node.

3. The efficiency of HTBIDS was tested based on parameters, namely Detection Accuracy (DA) and False Alarm Rate (FAR).

The organization of this paper is as follows. Section 2 represents the related work. Section 3 represents the network model. Section 4 represents the Attack model. Section 5 represents the proposed wok. Section 6 represents the Result and Discussion part. Section 7 represents the conclusion and future aspect of the proposed work.

2. RELATED WORK

Atakli et al. [9] have proposed a model that determines the trust of the sensor node using a weighing method and reduces overall communication between the sensor node and clustered networks. Jiang et al. [10] have established a model based on WSN distribution. Explicit trust and indirect confidence decide the confidence of the node in its model. For the measurement of direct trust, contact trust, energy confidence and data trust are seen as trust metrics. If the monitoring node cannot determine the trust value of the node, indirect confidence calculation based on the recommendation of the neighboring node. Jaydip et al. [11] have suggested mechanism of DRI table

and cross checking of DRI table, when detecting a black hole node in MANET using AODV. We found working legacy of AODV along with DRI and Cross-Checking process. Because of this, we will consider a safe path from the sender node to the receiver node against anomalous nodes.

At the time of network communication, the data routing is disturb due to attacks in the network. There are different attacks in the network such as black hole attack, wormhole attack, sinkhole, limited forward attack and Sybil attack [12].From the related research, we can find many methods for determining the confidence level of sensor nodes based on the confidence measurements. As per survey of related work, few techniques for detecting the periodic jamming attacks have been published on the concept of Data Routing Information (DRI) and Cross Check method. However, we have taken the direct trust and experiences of other nearby nodes into consideration when measuring the confidence of sensor nodes by using hop counting as confidential measurements. For further security purposes, at the time of transmission of the sensor node over the networks, we have also introduced DRI and Crosschecking methods.

3. NETWORK MODEL

The cluster contains a few Sensor Nodes (SN) and one cluster head (CH) controls it. This cluster has a variety of clusters. Within the network, a sensor node can send or receive data through several intermediate sensor nodes (SN) on its respective cluster heads (CHs). As normal, the combined data from the Base Station (BS) have been given to the Clustered Head (CH). The sensor node to the clustered head transmission scenario has been found [13].

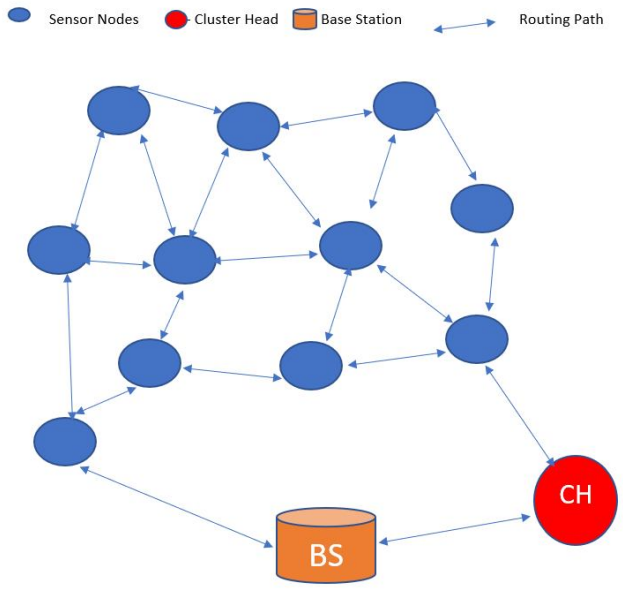

Figure 1: Clustered architecture for WSNs.

Here we have taken (Δt) as time period to update the trust.

Let $T_{ab}^{D}(t)$ Signifies the node-calculated direct trust factor *a* on node *b*during the time (t), and may be depicted as:

$$T_{ab}^{D}(t)=T_{ab}^{Phy}(t) \quad (1)$$

where $T_{ab}^{Phy}(t)$ signifies the trust value.

$$T_{ab}^{Phy}(t) = x_1.T_{ab}^{Ecm}(t) + x_2.T_{ab}^{Nmt}(t) \quad (2)$$

Here x1 and x2 are the weighting parameters with sum of both the parameters equal to one. The weighting parameters are generated randomly by the system. The trust of SN is checked regularly. Node 'a' here tests the trust of node b at (Δt) time.

The final confidence of node 'a' on node b's is:

$$T_{ab}(t)=\gamma T_{ab}(t-\Delta t) + (1-\gamma)T_{ab}^{D}(t) \quad (3)$$

Where $T_{ab}(t-\Delta t)$ = Past trust value of node a on node b *and* $\gamma \in [0,1]$= Weighting value of the previous total trust value. The confidence value measured has a higher importance than the trust value of the past. Therefore, γ can be presented as $(x^{-\Delta t})$, where *x* is exponential function.

4. ATTACK MODEL

The periodic jamming attack in the physical layer is the popular attack in which the signals are of short duration and are transmitted periodically. All other communications are interrupted by these transmissions. This leads to a denial of service, where a true node accepts messages and rejects other services. The model of the attack can be interpreted as follows: I = EI+MI, where I is the information that may be true or false depending on the device, the predicted information is EI, and the malicious information is MI.

The energy consumption equation can be expressed as $I_{Ecm} = EI_{Ecm}+MI_{Ecm}$,

where I_{Ecm}=Complete energy absorbed by the node in particular time, EI_{Ecm}=The estimated energy consumed in time by the monitored node and $MI_{Ecm=}$ The extra energy consumed by a node (malicious / real) [14].

5. PROPOSED WORK

In this proposed method, first we calculate the trust of each sensor node by trust evaluation method over cluster network. After that, all trusted nodes are again checked by DRI and Cross checking method. Finally, clustered head gets the genuine node through this process and transmits the data from genuine nodes to destination node.

A. Trust Calculation of Sensor Node at Physical Layer

Energy consumption(Ecm) and transmission message number (Nmt) are known to be the confidence indicators in the physical layer. This is reflected primarily in the transmission and receipt of bits. This refers to a node's energy consumption. Normally abnormal node submits or receive additional packets leading to increased energy consumption. Therefore, we took Ecm and Nmt as the basic confidence calculation parameters at the physical layer. During the time period (Δt), Node 'a' measures the energy expended by the next node 'b'. Node 'b' has a relative deviation RD_{Ecm} from the energy usage (Ecm) and is defined as follows:

$RD_{Ecm}=\frac{\Delta Ecm_b(t)-\overline{\Delta Ecm(t)}}{\overline{\Delta Ecm(t)}}$(4)

Where,$\Delta Ecm_b(t)$ is the consumed energy of node 'b' during time periodΔt.

$Ecm_k(t) = N_t * E_{trans}$(5)

Where, N_t is the number of messages transmitted and E_{trans} is the energy required to transmit the message. This allows energy consumption to be measured as follows [10]:

$E_{trans} = P_{trans} * \frac{Packet\ Size}{Data\ Size}$(6)

Where, $\overline{\Delta Ecm(t)}$ is the mean of energy consumed during the time span by neighboring nodes, 'a' and 'm' is the number of neighboring nodes. As a node of communication, the energy consumption is calculated by node 'a' in time periodΔt.

$\overline{\Delta Ecm(t)} = 1/m \sum_{a=1}^{m} \Delta Ecm_a(t)$(7)

The nodal trust decreases when the Ecm variance increases. So, we quantify the physical trust as:

$$T_{ab}^{Ecm}(t)=\begin{cases}1-RD_{Ecm}(t), if 0<RD_{Ecm}(t)<1\\ 0, RD_{Ecm}(t)\geq 1\\ 1, RD_{Ecm}(t)\leq 0\end{cases} \quad (8)$$

In this above equation (8),the variance will be the smallest or equal to zero, if the node 'b'has less Ecm than the mean energy consumption and the node 'b' is accurate. The Ecm of node 'b' is twice the normal Ecm ifnode 'b'is considered as malicious and RD_{Ecm} is greater than or equal to 1. The trust T_{ab}^{Nmt} is considered as the trust parameter. The node 'a'detects the transmission of node 'b'. It monitors the Nmt of node 'b' during (Δt), which is represented as $x_{ab}(t)$. The mean is represented as$\overline{x(t)}$ and it is shown as follows:

$\overline{x(t)}=1/n \sum_{l=1}^{m} x_{al}(t)$(9)

$x_{al}(t)$ represents the Nmt of node *l* during (Δt), where node *l* is the neighbor node of node 'a'.The deviation of Nmt of node 'b' is calculated as:

$RD_{Nmt}(t)=\frac{Z_{ab}(t)-\overline{Z_{ab}(t)}}{\overline{Z_{ab}(t)}}$(10)

The number of message transmission (Nmt) with trust T^{Nmt} can be calculated as:$T_{ab}^{Nmt}(t)=\begin{cases}1-RD_{Nmt}(t), if\ x_{ab}(t)>\overline{x_{ab}(t)}\\ 1, else\end{cases}$(11)

If the Nmttrust metrics of sensor node 'a' is greater than the mean ofNmt trust value is decreases [14].

B. DRI and Cross-Checking Method

We have introduced Authentication and Reliability concepts into this method. Through our algorithm, we check the status of "node authentication" and "path authentication" in the network and the list of already authenticated nodes is kept. We have also used the concept of "Public key sharing" with the neighbouring nodes; to locate the reliable nodes in the communication by keeping the shared key list. We have proposed key-sharing principles for secure communication, transmitting malicious notices after finding abnormal nodes. The proposed system helps to keep the data transmission within nodes in WSN [15].

C.Hybrid Trust Based Intrusion Detection

In HTBIDS-DC, here we have taken two types of method for detecting malicious node and checked twice for detecting the genuine node. In the first method, each sensor node is evaluated the trust value by the deviation of key factor at physical layer with the help of their neighbouring node. Finally, untrusted node is treated as malicious node. On the second method, all trusted nodes broadcast the RREQ message to its next trusted node. Each node maintains a DRI table and Reliable List. If the trusted nodes are present in the DRI and RL then passes to the next node otherwise discarded the transmission process. Further, this process is continued up to destination node.

The proposed algorithm is stated as follows:

HTBIDS(TS_Node, D_Node**)**
Input:
TS_Node← Trusted Source Node
Dst_Node← Destination Node
Output:
M←Malicious Node

1. *TS_Node broadcasts RREQ message.*
2. *Each node 'A' in the network(N) maintains a DRI Table (DT) having the information of Node_Id and Sharable_Key of the nodes whose RREQs or RREPs are passing through 'A'.*
3. *Each node 'A' in the network(N)maintains a Reliable List (RL) by considering the frequency of messages passing through 'A'.*
    a. *The nodes sending frequently through 'A' are present in RL (A).*
    b. *Otherwise, the nodes are not present in RL (A).*
4. *The RL (A) is updated as per the changes in DT that is dynamic in nature.*
5. *An authentic path between TS_Node and Dst_Node is established through the following steps:*
    a. *After receiving RREQ message from TS_Node, Dst_Node sends RREP message to TS_Node by the same path of the first receiving RREQ message but in a reverse direction.*
    b.
        i. *If Dst_Node is listed by TS_Node in its RL then the Dst_Node is proved to be authentic and message is received. Set M←0.*
        ii. *Else Dst_Node is considered as malicious node and broadcasted over the network N. Set M←Dst_Node.*
6. *Return (M)*

As per above algorithm, we have claimed that the HTBIDS-DC is giving better performance than others Intrusion Detection System in WSN with respect to DA and FAR.

6. RESULTS AND DISCUSSION

We have studied output in Matlab R2015a of the scheme we proposed. The periodic jamming attack is introduced by adding additional messages to the estimated number of receiving messages. A uniform random distribution function produces the number of messages sent by a malicious node in a particular time period. It is generated for normal nodes from 20 to 30 messages, and for malicious nodes from 20 to 50. The final confidence is then calculated according to the proposed IDS model. The parameters considered for analysis are shown in Table 1.

Table 1: Performance Analysis Parameters

Parameters	Values
Network Size	100 x 100 m2
Cluster Head	01
Density of Sensor nodes	20,40,60
Communication Range	30m
Packet Size	10 bytes
Data Rate	512kbps
Routing Protocol	AODV
Number of Runs	10
x1, x2	0.5,0.5
Counting of Iterations	10

Our proposed scheme's output is calculated by different criteria, such as Detection Accuracy (DA) and False Alarm Rate (FAR).

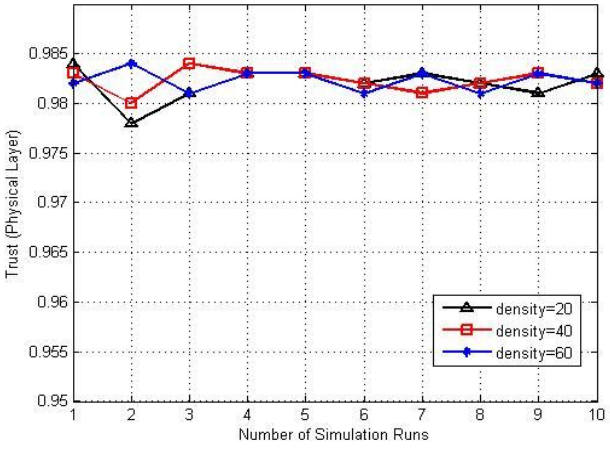

Figure 2: Trust value

Figure 2. shows that the average trust value of the network is constant when the number of simulations is increased. However, the simulation run between 0,977–0,984 fluctuates, because of less accurate data, between [0,977–0,984].

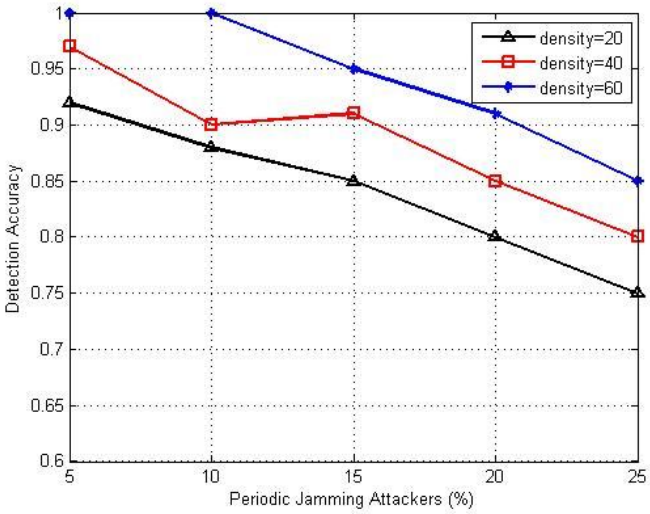

Figure 3: Detection accuracy

The relation between the number of periodical jamming attackers and detection accuracy is shown in Figure 3. The figure shows that the detection sensitivity decreases if the number of daily jamming attackers is higher. The detection precision is also observed as the network density increases.

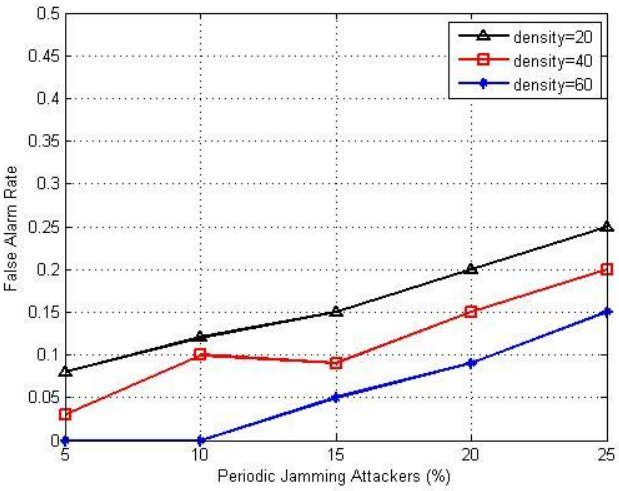

Figure 4: False alarm rate

The relation between the number of periodic jamming attackers and false alarm rate is shown in Figure 4. The figure shows that the rate of false alarm rises as the number of frequent jamming attackers rises. As the network density increases, the Distance decreases because the data is greater.

7.CONCLUSION AND FUTURE WORK

The proposed HTBIDS system detects periodic jamming attack of the Network. The results show that the average DA is 84%, 88.6%, and 94.2%, respectively, at density 20, 40, and 60. The average FAR is 15.8 percent, 11.4 percent, and 5.8 percent, respectively, at density 20, 40, and 60. Therefore, it is observed from the tests that when the density

rises, DA rises and FAR decreases. This method may be incorporate with Internet of Things (IOT) in future aspect. So that it can build a safe and secure IDS for back-off manipulation attack, wormhole attack, sinkhole attack, flooding attack, gray hole attack and selective forward attack.

REFERENCES

[1] M. Tiwari, K.V. Arya,R. Choudhari and K. S. Choudhary, "**Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information**", *Fourth International Conference on Computer Sciences and Convergence Information Technology*, 2009

[2] E. Nam Huh and T. Hong Hai,"**Light weight Intrusion Detection for Wireless Sensor Networks**". *Intrusion detection System*, Book chapter, Intech publisher,China, March 2011

[3] J. Du and J. Li, "**A Study of Security Routing Protocol for Wireless Sensor Network**", *International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 2011

[4] F. Bao, I. Chen, M. Chang and J. Cho,"**Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection**", *IEEE Transactions on Network and Service Management*, June 2012

[5] A. D. Wood and J.A.Stankovic," **Denial of Service in Sensor Networks**", *Computer*, Vol. 35, no. 10, PP. 54-62, Oct. 2002

[6] O. Depren, M. Topallar, E. Anarim and M.K. Ciliz, "**An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks"**, *Expert systems with Applications*, Vol. 29, no. 4, PP. 713-722,2005

[7] M. A. Rassam, M.A. Maarof and A. Zainal, "**A Survey of Intrusion Detection Schemes in Wireless Sensor Networks**", *American Journal of Applied Sciences*, 2012

[8] F. Bao, I. Chen, M. Chang and J. Cho, "**Trust-based intrusion detection in wireless sensor networks**",*In Proceedings of the IEEE International Conference on Communications*, Japan,June 2011

[9] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku and Z. Su, "**Malicious node detection in wireless sensor networks using weighted trust evaluation**", *In Proceedings of the Spring simulation multiconference. Society for Computer Simulation International*, PP. 836-843,April 2008

[10] J. Wang, S. Jiang and A. Fapojuwo, "**A Protocol Layer Trust-Based Intrusion Detection Scheme for Wireless Sensor Networks**", *Sensors*, Vol. 17, no. 6, 1227, 2017

[11] J. Sen, S. Koilakonda and A. Ukil, "**A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks**", *Second International Conference on Intelligent Systems, Modelling and Simulation*, 2011

[12] B. Kannhavong, H. Nakayama, Y. Nemoto and N. Kato,"**Security In Wireless Mobile Ad Hoc And Sensor Networks**" *IEEE Wireless Communications*, October, 2007

[13] U. Ghugar and J. Pradhan, "**ML-IDS: MAC Layer Trust-Based Intrusion Detection System for Wireless Sensor Networks**", *Computational Intelligence in Data Mining*,Springer, PP. 427-437, 2020

[14] U. Ghugar, J. Pradhan, S. Bhoi, R. Sahoo and S. Panda, "**PL-IDS: Physical layer trust based intrusion detection system for wireless s sensor networks**", *IJIT*, Springer, Vol. 10, no. 4, PP. 489-494, December 2018

[15] C. Khetmal, N. Bhosale, U. Ghugar and B. R. Bag, "**BADS-MANET: Black Hole Attack Detection System in Mobile Networks Using Data Routing Information (DRI) and Cross-Check Mechanism**", *The Role of IoT and Blockchain Techniques and Applications*, Apple Academic Press & CRC Press,In Press-April 2021