ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

Detection of Packet Dropping Attack in Wireless Sensor Network

Pitchammal @ Uma C[1], Dr. G. Ravi[2]

[1]Research Scholar in Computer Science, [2]Associate Professor & Head
Department of Computer Science, Jamal Mohamed College (Autonomous)
(Affiliated to Bharathidasan University)
Tiruchirappalli 620 020, Tamil Nadu, India
[1]uma.ayirathan1@gmail.com, [2]ravi_govindaraman@yahoo.com

Abstract: Wireless Sensor Network consists of a huge number of sensor nodes and latest advance is in wireless communications and it serves a backbone for controlling the real time applications. Wireless Sensor Networks are powerless to numerous kinds of the security fear which can decrease the performance of network and cause the sensors to send unacceptable data to destination. Designing a new wireless sensor node is enormously tricky task and involves evaluating a number of dissimilar parameters required by the target application. When accessing the internet or any network, little units of data called packets are sent and received. When one or more of these packets stop working to reach its intentional destination is packet loss. For users, packet loss manifests itself in the form of network interruption, slow service and even overall loss of network connectivity. The hostile node in the network is functioning as an attacker node and it takes all the information packets which are distributed through them. In this research work, we propose an intrusion detection system algorithm against the packet loss. The intrusion detection system is one of the probable solutions to make a wide range of security with attacks in WSN. The intrusion detection system can identify the abnormal nodes and improve it with the help of intrusion detection algorithm.

Keywords: Wireless Sensor Network, Intrusion Detection System, Security, Malicious Attacks, Packet Loss.

I. Introduction

A rising technology is Wireless Sensor Network where sensors are organized at extreme geographical locations where human interference is not possible. The Wireless Sensor Network consists of sensor nodes clustered into one network. They are located at different geographical locations and data can be composed with ease, the major reason of WSN growing quickly is the sensor nodes between the network that do not need physical infrastructure and can be located at extreme environmental conditional where human interferences are not possible The data transferred through the sensor nodes are mainly used in crucial decision making process. Since WSN is a wireless infrastructure it attracts the attackers to corrupt/misuse the data. A special type of Wireless sensor networks that work in decentralized environments are MANETs where in every node is competent of forwarding the data to its neighbor within the frequency range which ultimately transfer the data to the specific destination. The data transferred play a significant role key in terms of decision making processes if they belong to huge scales networks. Hence the data needs to be transferred with greatest security. In similarity to Wired networks, Wireless nodes are more prone to attacks such as DOS, wormhole, Tunneling, Sybil, Traffic analysis, all these attacks show the way to Packet drops within the network, which indirectly affects the packet delivery ratio, extra energy consumption and a smaller amount throughput [1].

The nature of wireless sensor networks (WSNs) makes them very susceptible to adversary's malicious attacks. Therefore, network security is a significant issue to WSNs. Due to the restrictions of WSN, intrusion detection in WSNs is a challengeable job. An intrusion detection system (IDS) monitors a host or network for mistrustful activity patterns outside normal and predictable behavior. Presently, there are a number of research efforts on intrusion detection for WSN. Predetermination of the position of sensor nodes is not compulsory. This feature allows us to use these networks in regions which are not available or in the relief operations throughout disasters. WSN is vulnerable due to two main reasons: 1) they use broadcasting for data transmission and due to this reason are more vulnerable to different kinds of security attacks. 2) The nodes sometimes are located in non-safe environments where much protection is not accessible to them [2]. Due to several intrinsic features of WSN, it is not easy to perform efficient intrusion detection in such a resource-restricted environment. Numerous intelligent or statistical approaches are too difficult for WSNs. The main factor that has an effect on the packet loss ratio is unobservability and security inside the network to avoid illegal access of data /packet at the same time as transmitting to other nodes.

II. Related Work

Ruirui Zhang et al.,[3] proposed a negative selection algorithm based on a spatial partition and applied to hierarchical wireless sensor networks. The algorithm first examines the sharing of self-set in the real-valued space, then divides the real-valued space, and numerous subspaces are obtained. Selves are filled into dissimilar subspaces. The negative selection algorithm implemented in the subspace. The results demonstrate that the model has improved with time efficiency and detector quality, saves sensor node resources, and decreases the energy consumption.

Mnahi Alqahtani et al.,[4] proposed a new model to identify intrusion attacks based on a genetic algorithm and a great gradient boosting (XGBoot) classifier, called GXGBoost model. The gradient boosting model designed for improving the performance and to recognize minority classes of attacks in the enormously unfair data traffic going on wireless sensor networks. A set of experiments was performed on wireless sensor network-detection system dataset using holdout and 10 fold cross validation techniques. The outcomes of 10 fold cross validation experiments found that the proposed approach outperformed the state-of-the-art approaches and other ensemble learning classifiers with high detection rates [3].

Hongchun Qu et al.,[5]. proposed a lightweight intrusion detection method that was capable to frankly map the network status into sensor monitoring data acknowledged by the base station, so that the base station can sense the anomalous changes within the network. Their method is highlighted by the combination of fuzzy c-means algorithm, one-class SVM, and sliding window procedure to efficiently differentiate network attacks from anomalous data. Experiments demonstrate that this method can not only discover anomalies, but also discover whether anomalies are network attacks, which is more practical than most anomaly detection algorithms.

Opeyemi Osanaiye et al., [6] proposed an approach using a statistical process control technique to identify these attacks. At this point, an exponentially weighted moving average (EWMA) to identify inconsistent alterations in the strength of a jamming attack event through packet inter-arrival feature of the expected packets from the sensor nodes. Results show that proposed method can proficiently identify the occurrence of a jamming attack with slight or no overhead in WSN.

Imeh Umoren et al.,[7] proposed practical congestion detection control simulator that imitates and optimizes packets dropping in a WSN. The proposed work permits for the determination of the system's reliability from factors that prompts congestion resulting in packets dropping. The factors considered numeral packets, throughput, packet delivery ratio, error rate and delay.

Prathap U et al.,[8] proposed a technique to identify malevolent nodes, which execute selective packet modification and dropping. Any successive three nodes on the routing path secure the 2-hop channel with the sharing of polynomial based triple key. A node encrypts the packet with a triple key shared with 1-hop and 2- hop nodes, monitor the packet forwarding from 1-hop node and decides the malevolent activity of the 1-hop node. Simulation results demonstrate that proposed method identifies the malevolent nodes proficiently and early. The proposed method is effectual to identify selective dropping and modification attacks compared to CRS-A and SFAD2H approaches.

III. Proposed Methodology

The main factor that has an effect on the packet loss ratio is unobservability and security in the network to avoid unofficial access of data/packet while transmitting to further nodes. The unobservable routing protocol is accomplished using two scenarios:

Scenario I: Attack by malicious node in the network causing packet drop

Step 1: Deployment of nodes
Step 2: Topology Creation
Step 3: Communication among nodes
Step 4: Path selection
Step 5: Data transfer among selected nodes from source (s) to destination (d)
Step 6: Dropping of packets by malicious node from the adjacent node

Scenario II: Selection of secure route to shift data from source to destination with no attack (Packet drops). It will check every node by communicating with the other, and then select secure path for data transfer from source to destination.

Wireless Senor Network has two kinds of nodes: sink nodes and sensor nodes. The sink (or base station) is an influential node that behaves as a boundary between the sensor nodes and the clients of the network. The sink allots the data from sensor nodes occasionally. The sensor nodes have the capability of sensing the neighboring environment. Sensor nodes will produce sensor data and data packets. Beacon node is a node that has their position information.

Assume that N nodes in the network. Assume that the number of the malicious nodes is M ($0 < M \ll N$).

S_n – Source node
S_i – Set of sender sensor node
S – Sink node
I – Identity List
L_c – Local Cache
D_i – Set of Identity of S_i
ΔT_V – Trust Value
F_c – Failed Transfer Collection List

I. Path Construction:

A) General Path

Algorithm1: Packet Transmission without Malicious Nodes

```
(1) A source node ($S_n$) sends a data packet to sink node ($S$).
    a) To each data packet, $S_n$ adds an empty list to the
       Identity List (I).
    b) Initially the Local Cache($L_c$) will be empty
(2) When a sensor node ($D_i$) receives a packet
    a) If it is a normal node, it adds its identity ($D_i$) to I.
       where $D_i = \{d_1, d_2,...,d_n\}$
(3) If the packet arrives,
    a) $S$ extracts $I = \{d_1, d_2,...,d_n\}$
       where $d_i$ refers to the identity of a sender sensor
       node $S_i$
    b) For every packet transmission the rate of success
transmissions will be added into $L_c$
    c) $S$ adds I to a notification packet and sends the packet
to $S_n$ for reference.
    d) Once the notification arrives, $S_n$ extracts it and stores
into the list (I)
(4) When a sensor node ($S_n$) receives the notification packet
successfully, it will be declared as success packet
transmission without any packet drops.
    a) If the packet is successfully transferred $L_c$ and I will
be reset.
```

B) Malicious Path

In the above general path algorithms, it is an supposition that if a data packet transferred from a source node profitably arrives at the sink, the path from the source to the sink is more likely to be secure for consecutive data communication. If the data packet is unsuccessful to reach the sink, it means that there is a malevolent node on the path from the source to the sink. According to the general path, we attach each normal path with a trust value ΔT_V. If the trust value reduced as zero or negative value, that path will be detached from the local cache of sensor nodes (such a detached path is said as malicious path).

Algorithm2: Packet Transmission with Malicious Nodes

```
(1) A source node ($S_n$) sends a data packet to sink node ($S$).
    a) To each data packet, $S_n$ adds an empty list to the
       Identity List (I).
    b) Initially the Local Cache($L_c$) will be empty
    c) Attach trust value $\Delta T_V$
         $\langle S_n, I, \Delta T_V \rangle$, check its trust value at time slot $t$.
(2) If $\Delta T_V > 0$, use the path for data transmission and
proceed the following steps (i), (ii) and (iii)
    (i) When a sensor node ($D_n$) receives a packet
        a) if it is a normal node, adds its identity ($D_{n(N)}$) to I.
           where $D_{n(N)} = \{d_1, d_2,...,d_n\}$
    (ii) If the packet arrives,
        a) $S$ extracts $I = \{d_1, d_2,...,d_n\}$
           where $d_i$ refers to the identity of a sender sensor
           node $S_i$
        b) For every packet transmission the rate of success
           transmissions will be added into $L_c$
        c) $S$ adds I to a notification packet and sends the
packet to $S_n$ for reference.
        d) Once the notification arrives, $S_n$ extracts it and
stores into the list (I)
    (iii) When a sensor node ($S_n$) receives the notification
          packet successfully, it will be declared as success
          packet transmission without any packet drops.
      a) If the packet is successfully transferred $L_c$ and I
         will be reset.
(3) If $\Delta T_V \leq 0$, don't use the path for data transmission
      a) Analyze any packet drops occurs using rate of
transmission
```

b) Not to update the path into the local cache (L_c)

c) Mark the path as malicious path.

d) Add the malicious path to a failed transfer collection list (F_c).

IV. Experimental Result

The result provides adequate performance in terms of packet transmitted, packet delivery and packet drop ratio. The main metric for performance evaluation are (i) Packet transmitted, defined as the overall number of transmitted data packets sent from the source node to the destination. (ii) Packet delivery ratio, defined as the ratio of the number of effectively delivered data packets to the whole number of packets sent from the source node. (iii) Packet drop ratio refers to the probability that a malevolent node will drop a packet. In Simulation, the nodes are arbitrarily placed in localization with 44 nodes having 5 default malicious nodes which is higher than the existing algorithm nodes. By having high number of nodes in simulation our proposed model attains better performance. The execution time is decreased than the prior algorithm because of using notification mechanisms where the successful normal nodes are noted in the Local Cache which will be noticeable as proficient nodes for further transmission and the malicious nodes are stored in the Failed Transfer List for the reference that these nodes are malicious, not to use in future. The notification mechanism was very supportive to attain high performance.

The sample values for the parameter in simulation model are shown in the following Table I.

TABLE I
PARAMETERS AND ITS VALUES

Parameters	Value
Total Nodes	44
Number of malicious nodes	5
Initial trust value	1
Packet size	1024 bits constant
Packet drop ratio	0.2
Sensor Speed (X, Y)	2,2

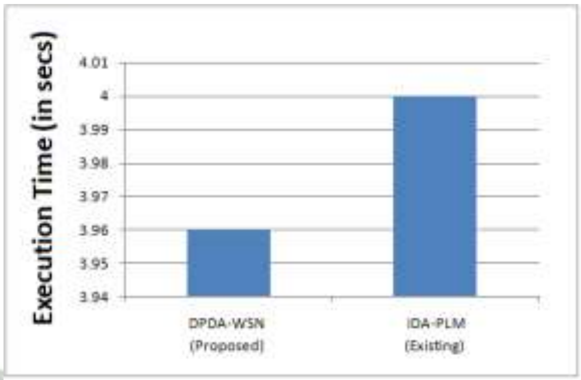

Fig 1. Comparison on Execution Time

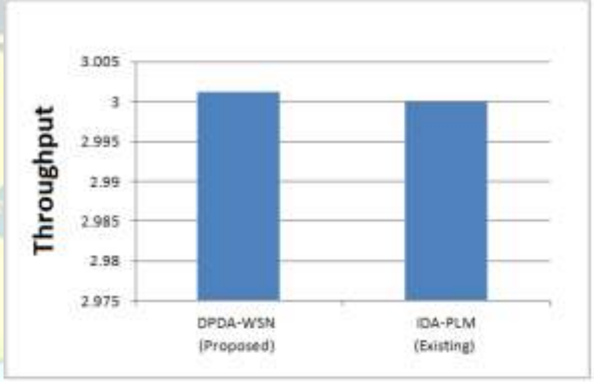

Fig 2. Comparison on Throughput

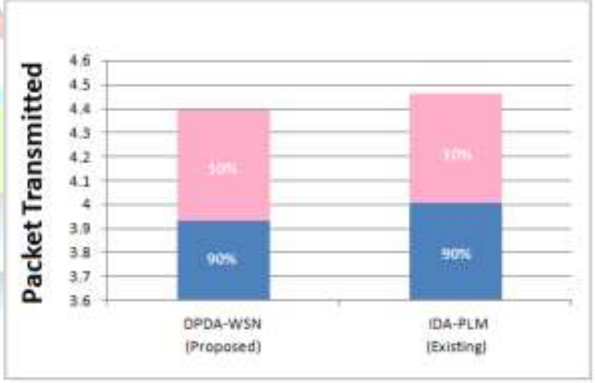

Fig 3. Comparison on Packet Transmitted

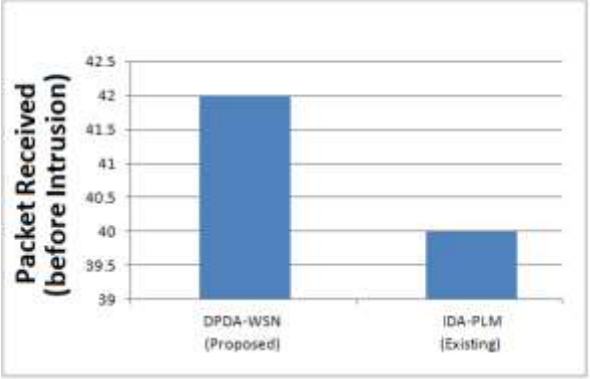

Fig 4. Comparison on Packet Received (before intrusion)

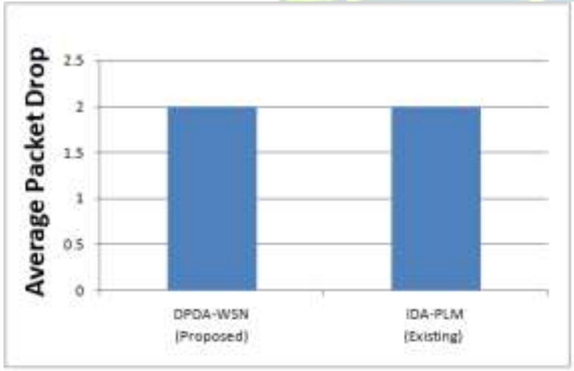

Fig 5. Comparison on Average Packet Drop

TABLE IIIII
RESULT

Results	*Proposed Algorithm* DPDA-WSN	*Existing Algorithm* IDA-PLM
Execution Time	3.95	4
Throughput	3.25	3
Packet Transmitted	90% in 3.95 seconds	90% in 4 seconds
Packet Received (before intrusion)	42%	40%
Average Packet Drop	2	2

Table II shows the performance report on proposed and existing algorithms which shows that the proposed algorithm DPDA-WSN is having better results on its performance than the existing.

V. Conclusion

Wireless sensor networks (WSN) are unified sensor nodes that commune wirelessly to gather data about the surrounding environment. The enclosure of wireless communication technology also acquires different types of security threats. Since security threats to WSNs are more and more being diversified and deliberate, an intrusion detection system is needed to evade packet dropping, data security from the intruders etc. The proposed algorithm will decrease the packet loss compare to the existing algorithm and it will develop the network performance with least execution time. Our simulation result explains that the execution time of DPDA-WSN is 3.96 seconds which is efficient than the existing one 4 seconds for 90% of packet transfer. The average packet dropping is 2 which are sustained equally as in existing algorithm. The proposed algorithm attains maximum throughput of 3.25 relatively to the existing algorithm throughput 3. With the simulation result it is confirmed that the proposed algorithm is more proficient than the exiting algorithm.

Our future work will extended by proficiently finding multiple alternating paths if any malicious node occurs while data transmission. We can also propose to find solutions for identifying other DoS attack, include as Sybil attacks and masquerading.

References

[1]. Miriam Lakde and Prof. Vaibhav Deshpande, “Analyze and Detect Packet Loss for Data Transmission in WSN”, Int. Journal of Engineering Research and Application, vol. 6, Issue. 9, pp. 01-04, Sep 2016.

[2]. Divyashree G, Durgabhavani A, KavyaM, Anushree Gudoor, Madhukar B Shetty, “Intrusion Detection System In Wireless Sensor Network”, International Journal of Recent Technology and Engineering (IJRTE), vol. 8, Issue. 1, pp. 2047-2051, 2019.

[3]. Ruirui Zhang and Xin Xiao, “Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division”, Hindawi Journal of Sensors, pp. 1-20, 2019.

[4]. Mnahi Alqahtani, Abdu Gumaei, “A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks”, Journal of Sensors, vol. 19(20), pp. 1-21, 2019.

[5]. Hongchun Qu and Libiao Lei, “A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks”, Hindawi Advances in Fuzzy Systems, pp. 1-12, 2018.

[6]. Opeyemi Osanaiye and Attahiru S. Alfa, “A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks”, Journal of Sensors, pp. 1-15, 2018.

[7]. Imeh Umoren and Daniel Asuquo, "Performability of Retransmission of Loss Packets in Wireless Sensor Networks", Canadian Center of Science and Education, Vol. 12, No. 2, pp. 71-86, 2019.

[8]. Prathap U, Deepa Shenoy P and Venugopal K R, "Detecting Selective Packet Droppers and Modifiers with Triple Key Distribution in Wireless Sensor Networks", International Journal of Applied Engineering Research, Vol. 13, No. 9, pp. 6926-6934, 2018.

[9]. Dai Jianjian and Tao Yang, "A Novel intrusion detection system based on IABRBFSVM for wireless sensor network", 8th International Congress of Information and Communication Technology, vol. 131, pp. 1113-1121, 2018.

[10]. W. Guo, Y. Chen, Y. Cai, T. Wang, and H. Tian, "Intrusion detection in WSN with an improved NSA based on the DE-CMOP," KSII Transactions on Internet and Information Systems, vol. 11, no. 11, pp. 5574-5591, 2017.

[11]. Syed Muhammad Sajjad and Muhammad Yousaf, "NeTMids: Neighbor Node Trust Management Based Anomaly Intrusion Detection System for Wireless Sensor Networks", International Journal of Computer Science and Information Security (IJCSIS), vol. 14, no.7, pp. 176-183, 2016.