International Journal of Advanced Science and Technology
Vol. 29, No. 11s, (2020), pp. 261-268

Enhance Routing Security And Network Lifetime In WSN Using Session-Based Aggregated Host Route Identification Algorithm

[1]R. Senthil Kumar, [2]Dr M Prakash

[1]Research Scholar, Dept. of Computer Science, VMKV Arts & Science College, VMRF Deemed University, Salem, Tamil Nadu, India.
[2]Research Supervisor & Associate Professor, Dept. of Computer Science, VMKV Arts & Science College, VMRF Deemed University, Salem, Tamil Nadu, India.

Abstract:

WSN unattended deployment of the physical environment of such sensor nodes that is vulnerable to harsh environments and attacks. Key management is the transmission of the most important wireless sensor network security data. In general, though routing of node-to-node communications is reduced in a secure data transfer network, regular routing and key management programs are shared keys installed on all neighbors of the sensor node. Routing protocols in sensor networks are designed not to focus on security, but to optimize limited resources. WSN's existing network layer security schemes can be generally divided into key management solutions and routing solutions. Dynamic Route scheduling approaches to the network some time affect the route source and destination node. The proposed solution to implement routing and aggregate data management for a large area WSN network. For secure routing, authentication of sensor nodes in the routing path is an important factor. The previous solution zone-based routing and key management to improve the network lifetime and performance. The Session-based Aggregated host Route Identification (SAHRID) algorithm to improve the routing security and the data collection protocol to collect the data from all the nodes. In this manner the network sends an approved 'HELLO' message to find the node and path trust value. Session-based Path Key helps to manage the data transfer and route identification or route stability of each session. The performance of SAHRID for analyzing 100 nodes is analyzed and calculating the ratio of packet transmission, network throughput, energy consumption, and average delay analysis. In this proposed method to improve the network route security and network parameters.

Keywords: *Aggregated node, WSN routing, session-based path key, SAHRID.*

I. INTRODUCTION

Wireless sensor networks are connected by monitoring wireless nodes for different sensors implemented in a physical environment. For military purposes used to monitor enemy movements, it is a measure of breeding yield and is used in the industry to measure various control parameters. It is operating on sensor nodes within a certain limited range of transmit power resources. Improve the energy performance of data transmission over WSN splitting and less retrofit network consumption. Providing Energy-Having an improved network destination node in the life cycle for efficient collection of data WSNs is multiple tasks. Efficient and effective data collection, and spans spatial-related improve the network lifetime and provide energy. A traditional data collection algorithm to reduce the number of connections based on multi-hop communication between WSN and energy balance sensor nodes. However, the data distribution ratio is not between sensor node WSN to improve network performance. Introduced to improve the throughput network, the amount of data collected from various sensors minimizes the power consumption during the shortest path node maximum technology. However, it does not consider the trade-off between energy consumption and the lifetime of the WSN network.

The authentication data, are sending and receiving nodes share a secret key to calculate the symmetric or asymmetric of the achieved message authentication code mechanism. The following factors are data in wireless sensor network certification that should be considered: Due to the nature of the unmanned sensor network, which is to ensure that wireless media and authentication become challenging tasks. And calculating sensor energies and deploying complex password restriction techniques can be impractical.

The security of the routing protocol depends on the location of the node and the encryption technology. Routing the protocol design is very complicated because every node in the sensor network acts as a router. They have energy and memory usage efficiency at the same time strong enough to withstand security attacks and node failures.

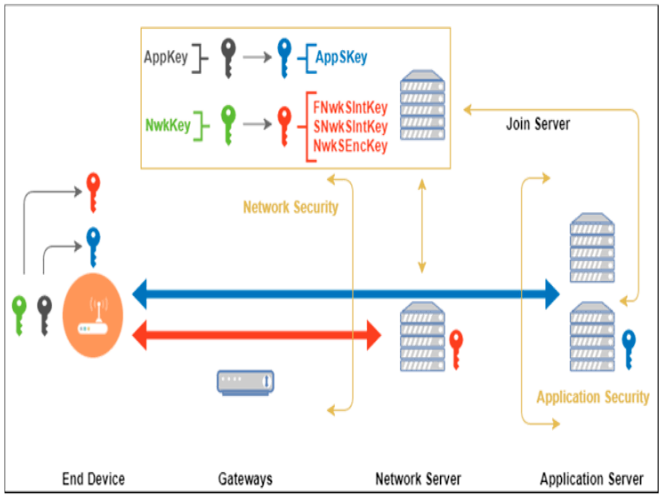

Fig: 1. key management system.

The first level of security provided is achieved by using one-way functions to ensure authentication and encryption key generation. The secure data transmission using the confidentiality and reliability of the MAC algorithm guaranteed by the protection scheme SAHRID communication. The program guarantees the flexibility and energy efficiency of various attacks.

II. REVIEW OF LITERATURE

In the author's analysis to detect integrated wireless network intrusions and integrated policies, network intrusions, network popularity, and detection information, detected signal models that create anomalous network traffic analysis models [1]. Network intrusions are on computer networks from unauthorized activity [2]. Therefore, an effective intrusion detection system needs to be established.

In general, intrusion prevention and intrusion detection have reached saturation, the most important issues in wireless sensor networks [3]. Trust computing sensor nodes for each major element of black hole attacks based on network layer deviations. A watchdog technique that relies on values for sensor node calculation periods by continuously monitoring adjacent nodes [4]. Gateway support vector machine intrusion detection anomaly detection method (SVM), intrusion detection for wireless sensor networks and deep learning techniques. Detection protocol, on-demand SVM classifier whenever a layered intrusion is suspected dynamically. Machine learning and statistical classification of malicious node locations [5]

The variety of offer sensor information, and this network is vulnerable to attacks on the natural environment and inherently unreliable transmissions, especially insider attacks. The key strategy is to use the integrated base stations to manage the WSN [6]. Establish conceptual nodes for

their different functions, and use the principal component analysis to optimize the V-detection algorithm and reduce the detection of the rules generated by the detection studies [7]. Performance of RBC-IDS, and adaptive machine learning-based IDS previously proposed: Mixed monitor and adaptive cluster IDS (ASCH-IDS). The results show that the same detection accuracy is achieved that ASCH-IDS, but the detection time of RBC-IDS [8].

To maintain security, IDS are widely used to prevent attacks by implementing appropriate internal trust-based mechanisms. However, in the age of big data, sensors can generate too much information and data, which reduces the effectiveness of trusted computing [9]. To address these issues, open a potential field between the sensor and the sensor first described between the intruders. Later, we developed a mobile mode sensor node and charge model using intruder points, which we recommend using the elastic collision model [10]. Malicious software attacks that publicly alter the dynamic characteristics of malware datasets are updated from system references. Deep Neural Network (DNN), a type of deep learning model, is exploring the development of flexible and effective IDS detection and classification of unexpected and unpredictable network attacks. It is necessary to change the behavior of the network and the rapid development of attacks, and will evaluate a variety of datasets generated in a static and dynamic way [11].

Efforts to ensure that wireless sensor networks (WSN) utilize the immune system, which is known as a dangerous technology. In other words, the multilevel intracellular detection system (IDS) is a function based on the designed immune cells. This is achieved by monitoring WSN parameters such as frequency and power enhancement, the size of the output data and the transmission of data and their weight concentrations, and IDS designs for wireless sensor network-based processes [12]

In that direction, it proposes the use of blockchain trust-based CITNs, which enhance their responsibilities, known as chains, to protect the integrity of shared information among peers and prevent intercepted internal attack cooperation [13]. And security. Keeping the synchronization protocol and putting CITNs ahead, this deal damages the trusted, trusted work chain in job verification, enabling joint IDS nodes to check mountain combinations [14].Multi-dimensional hierarchical trust Two sensor nodes (SNS) and cluster head (CHS) levels based on hop rating, fixed direct rating and interactive trust combined with feedback, honesty and trust and content proposal trust Consider the mechanism[15]. The evaluation of the SN trust by this means, the trust and evaluation of the CHS by the CHS, neighboring cluster heads and the BS did not evaluate in this way, the complexity of the evaluation reduces all other cluster heads in the network [16].

Seeing this challenge and presents under a hierarchical structure combines wireless intrusion detection flow sampling, which is based on Bayesian two-way trust management. In evaluations, performance in both analog and real-world network environment approaches [17]. In CITNs, challenge-based belief mechanisms are always considering possible solutions through the satisfaction of identifying malicious nodes. Based on the challenges of advanced CITN attacks, it is regarded as a passive love pointing the finger at some advanced news by gathering information and identifying passive requests as regular requests [18].

While offline, users are reporting the most relevant input capabilities for each type of detection by trained DNN-IDS intrusions. Each detection on the Internet reports that users contribute the most to the detection input function. The proposed method is perceived based on DNN-IDS KDD-NSL on datasets with multiple layers. Binary and multi-class classification datasets are performed. Also several DNN-IDS architectures with different depths to test to study the factors driving the classification. They provide a model for deep learning, normal system [20] behavior, and use exception-based network intrusion detection systems (IDS) to detect approaching anomalous behavior.

III. PROPOSED METHODOLOGY

A) Session-based Aggregated host Route Identification (SAHRID)

In this proposed approach to implementing in wsn for securely transfer data source node to the destination. Session-based Aggregated host Route Identification identifies the source and destination node on the network and calculates the trusted value each node. The session base re-key method based on the SAHRID proposes to introduce advanced security. Here to implement a data collecter it stores the node information and collects the data from all other nodes. Traditional connection-based data collection is used to reduce route failure and balance the number of multi-hop communication paths between WSN sensor nodes.

The proposed system SAHRID is shown in the block diagram Fig:2. The amount of data collected from various sensors minimizes the route management while the shortest path node maximum technology to improve the throughput network.

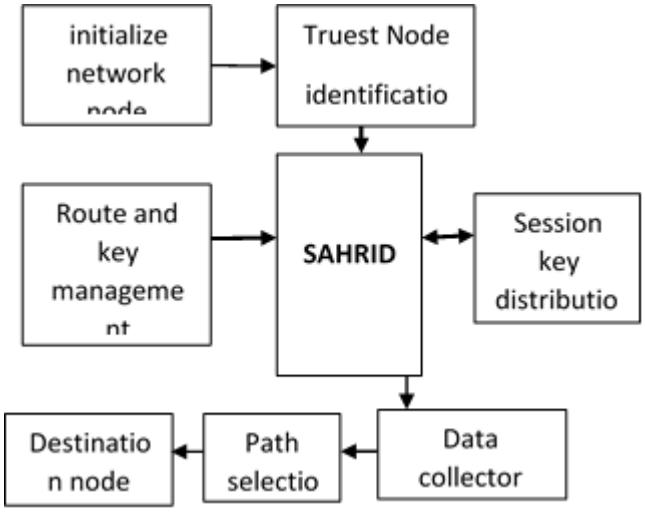

Fig: 2.Implementation of proposed SAHRID.

B) Data Aggregation Route and node selection

The route and node selection to apply the aggregation function all the node and choose the trust route. In this method using the elevation of a spatial and temporally relevant database for event-associated data from sensor nodes. Choose the data points used for the end delay and maintain the accuracy of data collection to minimize transmission. This reduction due to end delay is updated based on the spatial and temporal characteristics of events related to the size of the dynamically realized region.

Algorithm steps
Input : Initialize network node
Output: selective node (Sn)
While (node position and node Weight List)
Current Node ←Node ID- of - Least Weight of
the node(WL)
Neighbor list of Current node
{
(N1, N1-distance , N1-energy), (N2, N2- distance, N2-energy).... (Nn, Nn- distance, Nn-energy)
}

Current Node -WL = 1
Temp = WL++;
While (temp !=0)
If (Neighbor node ID- Status =is not alive)
Remove the first neighbor from Neighbor list
WLCount = WLCount – 1;
Else
Apply aggregate value Ag=$\sum_{n=o}^{node\ id}\{\sin^{-1} trust\ value + 1\ |Route\ id\}$
WLCount = WLCount - 1
End If
If (Ag==true)
Sn= $\lim_{n\to\infty}\left(node\ id + \frac{route\ value}{total\ number\ of\ route}\right)^n$
End if
End While
End While

C) Session key distribution

Each node in the wireless sensor network data communication, and all these data are combined into a sink node. Near the node to the base node plays a more important role because they are more complex when compared to regular nodes and routing protocols. Key pre-distribution schemes are fixed before they can be affected keys. in this session based key proposed by the key generation method provides a secure data transfer to the destination node for each session. When the first session data completely transferred to destination in the next transmission packet generated the new key based on route or source and destination path.

Algorithm Steps
Input: Selective node (Sn)
Output: Session Key ECK.
Initialize Key set ECK.
Identify the set of all routes available.
SS ← $\int \sum Sn \in Network$
For Each session Si from SS
Initialize node I'd SID.
Initialize node parameters.
Compute maximum bytes of packets to remain attached.
Ms ← $\int Max(routekey)$
Generate Key Ek ← Random (datapoint).
Compute the current size of the packets Cs ←$\sqrt{(Ms1 - Ms)}$
SID ← SID+MS+CS.
ECK ← {Ms, Cs, SID, EK}.
End

Above the algorithm generate the session key based on network source and destination path the steps are shown. First it will check the available paths in the network and read the all node id and its information then it will generate the session key.

IV. RESULTS

The proposed method Session-based Aggregated host Route Identification (SAHRID), the main process is to send the acquired information and the base node for further processing in the wireless sensor network environment. The resultant is processed with Network simulator NS2 with network area in 100 *100 m^2 with 100 nodes to transfer the data packets. The purpose of this SAHRID Algorithm is to determine from a random set of best-trusted paths and possible routing paths. The proposed SAHRID simulation result compares to existing method DTS-CBS, DSLR, and dZBGP.

The throughput ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node for a specified period.

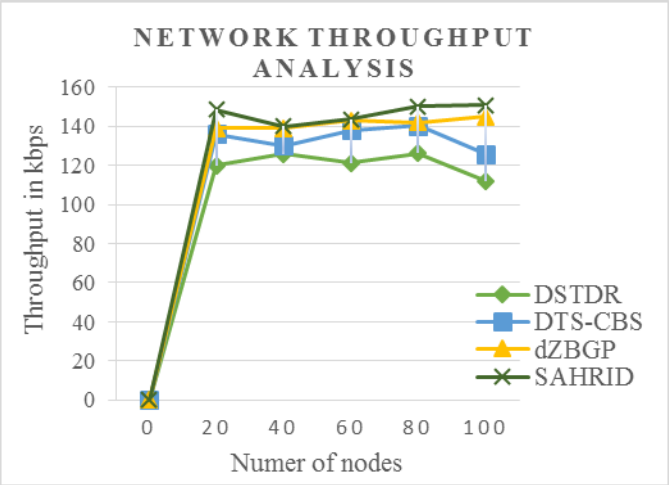

Fig: 3.Network throughput analysis.

Through experiments, we summarize the average throughput and running time of these four algorithms as shown in Fig:3. The proposed method SAHRID is compared with other existing methods DTS-CBS, DSLR, and dZBGP have high throughput 150.8Kbps for 100 number nodes.

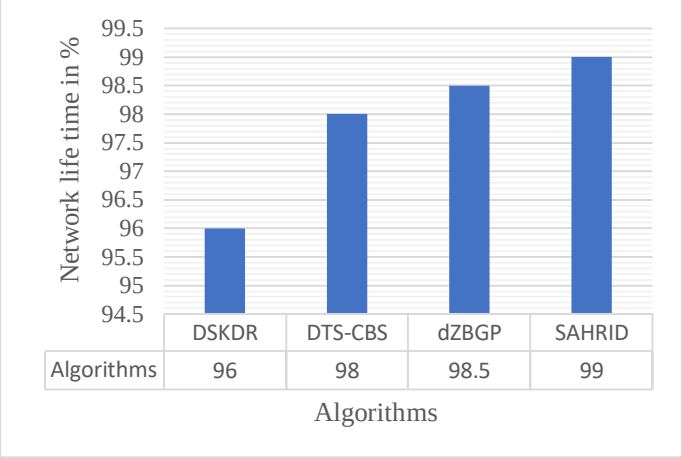

Fig: 4. Network Lifetime analysis

The Fig:4 shows the proposed approach SAHRID network lifetime compare to the existing method. In this result proposed approach more the 99% of a lifetime to achieve.

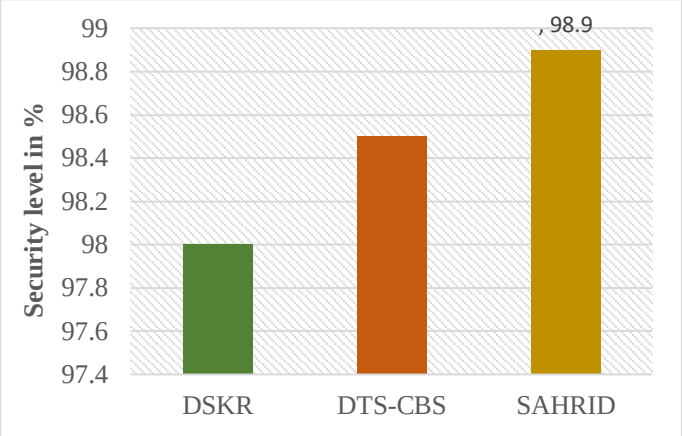

Fig: 5. Network Security analysis

Above the Fig:5 shows the proposed system simulation average security performance result. This proposed SAHRID algorithm is more secure than other methods.

The PDR is an analysis of the total number of receive packet divided by the total number of send packet. The proposed SAHRID PDR analysis result shows the Fig:6 it gives better PDR percentage compared to other methods.

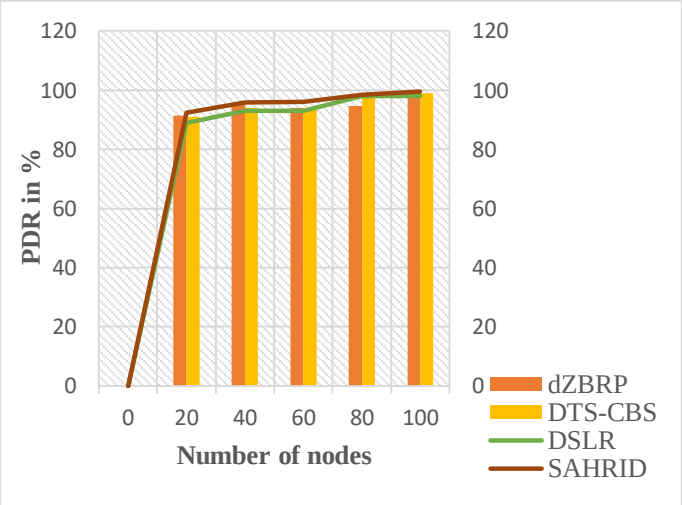

Fig: 6. network PDR Analysis

V. CONCLUSION

Wireless sensor networks are organized as a cooperating set of network nodes. After the deployment of wireless nodes, self-organize regular communication. In this proposed Aggregated synthetic data of data from various sources has been relocated to eliminate redundancy. Determines their active participation of direct communication path sensors based on which session key. Whether to check to retransmit the broadcast the session key, the proposed solution provides a mechanism for valid Re-keying. The simulation to evaluate the performance of the parameters like security analysis, throughput, delivery ratio. Further, to evaluate the practical performance of the proposed SAHRID algorithm based on simulation it gives better security and efficient communication in the network. In feature it needs to change the way for node failures and hidden terminal issues. Packets can send unnecessary data by reset. Therefore, this study can cover the problem of node and node failure with an extended solution. Localization issues and the potential for further expansion of payment solutions for wireless sensor networks as a result of technological advances should be addressed.

REFERENCES

1. Kapil Wankhade, Sadia Patka and Ravinndra Thool, "An efficient approach for intrusion detection using data mining methods", IEEE, 2013.
2. Umashankar Ghugar, Jayaram Pradhan "NL-IDS: Trust-Based Intrusion Detection System for Network layer in Wireless Sensor Networks" IEEE International Conference (PDGC-2018)
3. Medjak, D. Tandjani, I. Romdhani, N. Djdjig. "A Trust-based Intrusion Detection System for Mobile RPL Based Networks", IEE International Conference on IoT and IEEE GreenCom and IEEE CPSCOM and IEEE SmartData.-2017.
4. Pankaj Ramchandra Chandre ; Parikshit Narendra Mahalle ; "Machine Learning-Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification" 18 March 2019
5. YU Dunyi "Research on Anomaly Intrusion Detection Technology in Wireless Network"2018 International Conference on Virtual Reality and Intelligent Systems, pp - (540-543).
6. U Ghugar, J Pradhan, S.Bhoi, R.Sahoo, S Panda, "PL-IDS: Physical layer trust-based intrusion detection system for wireless s sensor networks", IJIT, Springer-2018.
7. Aymen Yahyaoui ; Takoua Abdellatif "Hierarchical anomaly-based intrusion detection and localization in IoT" 22 July 2019
8. Wang, J., Jiang, S., & Fapojuwo, A. O., "A Protocol Layer TrustBased Intrusion Detection Scheme for Wireless Sensor Networks". Sensors, 2017.
9. Meng, W., Li, W., Kwok, L.-F.: Towards Effective Trust-based Packet Filtering in Collaborative Network Environments. IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 233-245 (2017)
10. A. Shenfield, D. Day and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks," ICT Expr., vol. 4, no. 2, pp. 95-99, June 2018.
11. R.Sugumar, A.Rengarajan and C.Jayakumar, "Trust-based authentication technique for cluster-based vehicular ad hoc networks (VANET)", Wireless Networks-2018.
12. P. Li and W. H. Zhou, ''Hybrid intrusion detection algorithm based on k-means and decision tree,'' Comput. Modernization, vol. 37, no. 6, pp. 12–16, Dec. 2019.
13. Guo, Chen.I. Ray, Tsai, Jeffery J.P, " A survey of trust computation models for service management in the internet of things systems", Computer Communication-2017.
14. Q. Yuan and L. T. Lv, ''Network intrusion detection method based on a combination of improved ant colony optimization and genetic algorithm,'' J. Chongqing Univ. Posts Telecommun., vol. 29, no. 1, pp. 85–89, Jan. 2019.
15. Meng, W., Li, W., Xiang, Y., Choo, K.K.R.: A Bayesian Inferencebased Detection Mechanism to Defend Medical Smartphone Networks Against Insider Attacks. Journal of Network and Computer Applications, vol. 78, pp. 162-169, Elsevier (2017)
16. Tabatabaefar, M. Miriestahbanati, and J.-C. Gregoire, "Network ´ intrusion detection through an artificial immune system," in Systems Conference (SysCon), 2017 Annual IEEE International. IEEE, 2017, pp. 1–6.
17. N. Alsaedi, F. Hashmi, A. Sali,F. Z. Rokhani, " Detecting Sybil attacks in clustered wireless sensor networks based on energy trust system(ETS)", Computer communications-2017.
18. Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou and C. Wang, "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365-35381, May 2018.
19. H. Sadreazami, A. Asif and A. Mohammadi, "Data-adaptive color image denoising and enhancement using graph-based filtering," in Proc. IEEE International Symposium on Circuits and Systems (ISCAS), 2017.