International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Implementation of Security Protocol for Intrusion Detection Systems in Wireless Sensor Networks

[1]Amit Singh, [2] Dr. Devendra Singh
Department of Computer Science, IFTM University, Moradabad, Uttar Pradesh
[1]singh.amit013@gmail.com[2] devendrasingh@iftmuniversity.ac.in

Abstract— Sensor networks consist of compact sensors and actuators capable of monitoring physical conditions. Wireless Sensor Networks (WSNs) with limited power and dynamic topology require effective security mechanisms. Insider attacks pose a greater challenge than outsider attacks. This work proposes an Intrusion Detection approach in WSNs to detect attacks, emphasizing experimental results, parameter analysis, and Performance Evaluation based on accuracy and minimizing false positives.

Index Terms— Wireless Sensor Network, Security, Intrusion Detection System, Attacks.

I. INTRODUCTION

1.1 WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) have gained attention for their applications. A sensor network consists of nodes with sensing, processing, and communication capabilities to observe and react to events in an environment. These networks collect data on physical phenomena that were challenging before. WSNs include small sensor nodes densely distributed in an area and remote sinks forming a collaborative network. Nodes connect to other networks via gateways and collect environmental information. WSNs have important roles in military and civilian applications. Wireless sensor networks require specific properties, which include:

- Self-configuring: The network should facilitate easy deployment without manual configuration.
- Energy efficiency and robustness: The system should be designed to maximize the lifespan of the network by minimizing energy consumption and ensuring resilience.
- Latency-awareness: The network should prioritize delivering information to end-users as quickly as possible.
- Application-specific nature: The design and characteristics of the sensor network should align with the requirements of the particular application it serves.

1.2 WIRELESS SENSOR NETWORKS SECURITY

Sensor networks distribute small devices to detect changes in specific events. Security is crucial in wireless sensor networks (WSNs) to protect sensed data against various attacks. Security measures encompass confidentiality, authentication, integrity, privacy, non-repudiation, and anti-playback. Attackers can eavesdrop on radio transmissions, tamper with channels, or deploy malicious nodes for coordinated attacks. Tamper resistance is not universally applicable due to its cost in sensor nodes.

1.3 INTRUSION DETECTION SYSTEMS

An Intrusion Detection System (IDS) is a valuable yet underdeveloped service that detects and addresses potential compromises in network security. It serves as a secondary defense against attacks, safeguarding data integrity and system availability. IDS face challenges in resource-constrained, mobile wireless networks. By monitoring system events and comparing them to user profiles and emerging trends, IDS aims to detect intrusions and minimize false positives, enhancing detection accuracy.

II. MOTIVATION

An intrusion occurs when the fundamental elements of a security system, such as resource integrity and confidentiality, are compromised. Intrusion Detection Systems (IDS) act as a secondary defense against network attacks, particularly in sensor networks where internal nodes can be the source of intrusions. Authentication approaches play a vital role in securing the network and identifying intrusions through communication analysis. Energy conservation is also crucial in intrusion analysis, requiring protocol modifications to store historical information and optimize energy consumption.

OBJECTIVES

The objectives of the presented work are as follows:
1. Design a time-bounded communication history analysis approach for intrusion detection in sensor networks.
2. Enhance the DSR protocol to maintain communication history.
3. Conduct statistical analysis on communication parameters to identify effective communicating nodes.
4. Improve communication throughput and minimize data loss.
5. Implement the proposed approach in the NS2 environment.
6. Compare the results of applying and not applying an Intrusion Detection System to WSNs.

Wireless sensor networks (WSNs) are prone to physical attacks due to their exposed environments, limited resources, and shared wireless communication. Intrusion detection methods play a crucial role in identifying and securing against these attacks. Our system utilizes time-bounded communication history analysis to detect abnormalities in WSNs, ensuring security in applications such as military, medical, home security, and industrial automation.

III. RESEARCH METHODOLOGY

This research presents an improved approach for detecting network abnormalities through time-bounded communication history analysis. The study focuses on sensor networks, where energy-efficient communication is crucial. Identifying intrusion nodes or abnormal behavior in energy-constrained networks is challenging. To overcome this challenge, a protocol-level modification is proposed within the DSR protocol to minimize analysis time and communication overhead. Now the table information maintained by the DSR included some extra information listed below:

- Number of Requests processed
- Number of Replies Processed
- Average Time Taken
- Communication Count

The collected information is stored in a time-bounded history parameter, which is periodically cleared to maintain relevancy. During network communication, this information serves as a decision vector to identify effective nodes. The analysis focuses on different aspects, including comparing node processing time with a threshold to identify abnormalities, monitoring the number of replies from nodes to detect irregularities, and considering abnormal communication counts as potential signs of an attack.

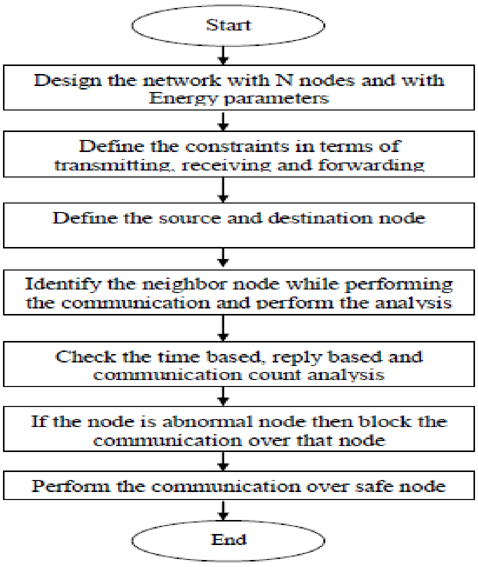

Start
Design the network with N nodes and with Energy parameters
Define the constraints in terms of transmitting, receiving and forwarding
Define the source and destination node
Identify the neighbor node while performing the communication and perform the analysis
Check the time based, reply based and communication count analysis
If the node is abnormal node then block the communication over that node
Perform the communication over safe node
End

Fig.1 Flow of Implementation and basic network design of the network

IV. APPROACH

To overcome the energy constraints in sensor networks, we propose an energy-efficient approach by modifying the DSR protocol. Our methodology involves analyzing network communication using time and communication vectors to detect and block malicious nodes, ensuring secure and reliable communication. The study is divided into two phases: modifying the protocol table to establish criteria and conducting communication analysis to identify compromised nodes. Safer paths are then utilized for secure transmission, reducing risks and optimizing network throughput.

V. ALGORITHM

```
Algorithm ()
{
1. Define a network with N nodes and specify their energy parameters:
i. Initial energy
ii. Transmission energy
iii. Forwarding energy
iv. Receiving energy
2. Define the source node (Src) and destination node (Dst).
3. Calculate the average response time of network nodes, denoted as AvgResTime.
4. Determine the average communication count over the network, denoted as AvgNetCount.
5. While (Src is not equal to Dst):
a. Identify the list of neighboring nodes to the source node (Src) and store them in a list called Neighborlist.
b. For each node i in Neighborlist:
i. If the response time of node Neighborlist(i) is greater than AvgResTime + Threshold, mark the node as a bad node.
ii. If the communication count of node Neighborlist(i) is greater than AvgNetCount + Threshold, mark the node as a bad node.
iii. Calculate the difference C between the reply count and request count for node i.
iv. If C is greater than the threshold, mark the node as a bad node.
c. Initialize EffectiveNode as 0.
d. For each node i in the network:
i. If node Neighborlist(i) is not marked as a bad node:
- If the throughput of node Neighborlist(i) is higher than the throughput of EffectiveNode and the delay of node Neighborlist(i) is lower than the delay of EffectiveNode, set EffectiveNode as Neighborlist(i).- Otherwise, if the throughput of node Neighborlist(i) is higher than the throughput of EffectiveNode, set EffectiveNode as Neighborlist(i).
- Otherwise, if the delay of node Neighborlist(i) is higher than the delay of EffectiveNode, set EffectiveNode as Neighborlist(i).
e. Set Cur as EffectiveNode.
6. End of algorithm.
}
```

The research aims to enhance existing intrusion detection schemes for effectively detecting insider attacks in wireless sensor networks. While cryptographic and authentication protocols provide protection against external intrusions, they are insufficient in detecting insider threats. Existing techniques focus on anomaly detection but lack specific intrusion detection capabilities. This work focuses on improving intrusion detection techniques to be applicable in all types of sensor networks, addressing the challenges that remain.

SIGNIFICANCE OF WORK

A Simple Intrusion Detection Algorithm (IDA) uses a database/usual behaviour as a basis for detecting all attacks. A database of signatures is created, or usual behaviour of network is recorded. Problem with preventive mechanisms is that they are able to prevent outsider attacks only, not insider attacks. And problem with misuse detection is that it does not detect any altered attack while anomaly detection detects the altered version of old attack, but it produces more false alarms. So in this research work, we are trying to detect the intrusions while minimizing the false positive alarms. The improved time

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

bounded communication history analysis approach having different parameters, is defined to identify the abnormality over the network. For example, military applications, medical monitoring, home security, industrial and manufacturing automation etc. are the fields, where security is required and this system can be used there to provide security.

VI. Basic Intrusion Detection Model

An Intrusion Detection System (IDS) consists of sensors or agents, a management server, a database server, and a console. The sensors monitor and analyze network activities, while the management server centralizes and analyzes the collected data. The database server stores the IDS data, and the console provides an interface for users and administrators. The IDS detects and alerts potential security breaches or suspicious behavior. It operates by gathering data from sensors, analyzing it on the management server, and generating alerts on the console. The database server stores the data for future analysis. Overall, the IDS components work together to monitor, analyzes, and responds to network security threats.

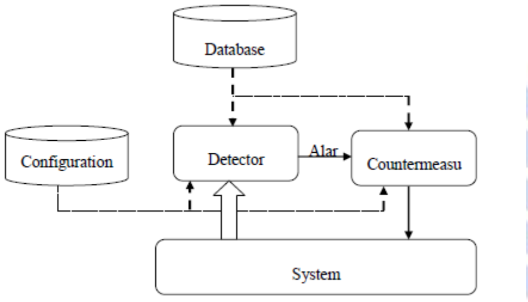
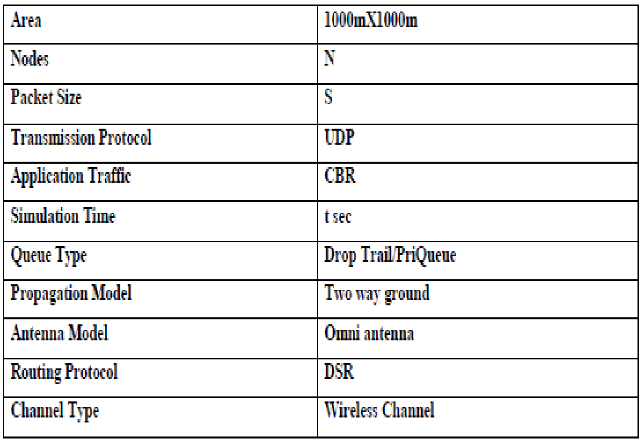


Fig. 2 Basic Intrusion Detection System Model

SIMULATION PARAMETERS

The basic simulation parameters associated with presented work are listed below:

Table-1: Simulation Parameters



Area	1000mX1000m
Nodes	N
Packet Size	S
Transmission Protocol	UDP
Application Traffic	CBR
Simulation Time	t sec
Queue Type	Drop Trail/PriQueue
Propagation Model	Two way ground
Antenna Model	Omni antenna
Routing Protocol	DSR
Channel Type	Wireless Channel

ANALYSIS PARAMETERS

The analysis parameters used in the presented work include:

1. Packets Received: The number of packets received in the network.
2. Packets Lost: Occurs when one or more packets fail to reach their destination.
3. Bytes Transferred: The amount of data transferred in terms of bytes.
4. Bit Rate: The rate at which bits are transferred from one location to another.
5. Last Packet Time: The time when the last packet in the network was sent.
6. Packet Delay: The difference in end-to-end one-way delay between selected packets.
7. Packet Loss Rate: The ratio of packet loss over a specific period of time.

Conclusions

Wireless sensor networks (WSNs) require strong security measures due to their limited resources and vulnerability to physical attacks. Attacks such as node capture and tampering pose a threat to the integrity and confidentiality of WSNs. To address this, intelligent intrusion detection methods are needed to detect and prevent such attacks. While cryptographic and authentication protocols have been proposed, they may not be sufficient to protect against all malicious attacks. Therefore, intrusion detection techniques focusing on anomaly detection will be studied and enhanced to provide better security. Implementing robust security measures is crucial to ensure uninterrupted network services in WSNs.

References

[1] "Wireless Sensor Networks", Technology Digest, Telecom Regulatory Authority of India, Issue 10, April 2012.

[2] A. Cerpa, J.Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical Model of Wireless Sensor Networks", IPSN, April 2005.

[3] Kiran Maraiya, Kamal Kant, and Nitin Gupta, "Application based Study on Wireless Sensor Networks", International Journal of Computer Applications (0975-8887), Volume 21-No. 8, May 2011.

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ISBN 89-5519-129-4, ICACT 2006, February 2006.

[5] Murad A. Rassam, M.A. Maarof and Anazida Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks", American Journal of Applied Sciences 9(10): 1636-1652, ISSN 1546-9239, 2012.

[6] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal of Communications, Issue 1, Volume 2, 2008.

[7] Keshav Goyal, Nidhi Gupta, and Keshawanand Singh, "A Survey on Intrusion Detection in Wireless Sensor Networks", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 2, Issue2, pp 113-126, ISSN 2278 – 0882, May 2013.

[8] Rodrigo Roman, Jianying Zhou, and Javier Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", 2006.

[9] Chee-Yee Chong, Member, IEEE and Srikanta P. Kumar, Senior Member, IEEE, "Sensor Networks: Evolution, Opportunities, and Challenges", Proceedings of the IEEE, VOL. 91, NO. 8, August 2003.

[10] Joseph Migga Kizza, “Implementing Security in Wireless Sensor Networks”, Data Communication and Computer Networks, pages296-310,2008.

[11] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid, and Pervasive Computing, 2006.

[12] Fereshteh Amini, Vojislav B. Misic, and Jelena Misic, “Intrusion Detection in Wireless Sensor Networks”, Security in Distributed, Grid, and Pervasive Computing, 2006.

[13] Vijay Bhuse and Ajay Gupta, “Anomaly Intrusion Detection in Wireless Sensor Networks”, Western Michigan University, Kalamazoo, MI-49008, USA, January 2005.

[14] Krontiris Ioannis and Tassos Dimitriou, and Felix C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks”, 2007.

[15] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami, “Intrusion Detection for Routing Attacks in Sensor Networks”, International Journal of Distributed Sensor Networks, 2: 313–332, ISSN: 1550-1329 , 2006.

[16] S. Sharma, “Energy-efficient Secure Routing in Wireless Sensor Networks”, Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.

[17] D. Boyle, T. Newe,”Securing Wireless Sensor Networks: Security Architectures”, Journal of Networks, 2008.

[18] X. Du, H. Chen, “Security in Wireless Sensor Networks”, IEEE Wireless Communications, 2008.

[19] Granjal, R. Silva, J. Silva, “Security in Wireless Sensor Networks”, CISUC UC, 2008.

[20] Jun Zheng and Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, a book published by A John & Sons, Inc, and IEEEE, 2009.

[21] E. Yoneki and J. Bacon, “A survey of Wireless Sensor Network technologies: research trends and middleware’s role”, Technical Report, 2005. http://www.cl.cam.ac.uk/TechReports, ISSN 1476-2986.

[22] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless sensor network security - a survey”, Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, 2007.

[23] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, “Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey” Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27.