IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

# Intrusion Detection System (IDS) with trusted nodes for improving security in Wireless Sensor Network

**S. Jawahar[1], J. Adamkani[2*]**

[1]Dept of MCA, Asan Memorial College, Chennai, India
[2]P.G. Dept of Computer Science, The New College, Chennai, India

**Corresponding Author: adam_kani@rediffmail.com*

**Available online at: www.ijcseonline.org**

Accepted: 14/Oct/2018, Published: 31/Oct/2018

***Abstract*-**Wireless Sensor Network (WSN) are the emerging and challenging technology with low processing and battery power. Security becomes a major issue in WSN; because of its wireless nature it is prone to various types of attacks and losing of data packet. Secure routing is important to avoid this type of issues. They are many techniques are available to provide secure routing to WSN. In the proposed work, our main aim is to find the trusted node and routing is done through the node to provide secure routing. The trusted node is identified by using Hidden Markov model (HMM) and it is rated. And also giving the un trusted node a chance to relay prove its identity. It provides the security features with minimum overhead and energy efficiency. The performance of proposed approach is illustrated that proposed model performs effectively compared with other existing approaches. Results demonstrated that developed HMM with trusted node provides significant performance in terms of memory overhead, delay, and Packet delivery ratio and energy consumption.

***Keywords*-** WSN, HMM, Trusted Node, Attacks, Routing, Intrusion Detection System.

## I. INTRODUCTION

Development of wireless sensor networks (WSN), offers the promise solution for monitoring critical infrastructure, it have been proposed for applications such as traffic monitoring, building monitoring, health care and battlefield surveillance[1] . In any application using critical infrastructure, there is a risk of malicious attacks on this infrastructure, this attacks can used for a terrorist act or as a financial gain. Security is a vital requirement in these networks and it must be established according to their constraints to can solve weaknesses and vulnerabilities of these networks. In this paper, we investigate how to incorporate intrusion detection into wireless sensor networks, and present a new approach based on mobiles agents to detect intrusions on WSN. A key attraction of sensor networks is their ease of installation and operation.

However, security is one of the key challenges to creating a robust and reliable sensor network [2]. Security is faced with additional challenges due to complexities such as an unreliable node operation, an unpredictable node movement and a wireless access medium. These challenges make a very important potential to exploit weaknesses in the WSN. Consequently, Intrusion Detection Systems (IDSs) are required to detect both known security exploits and even novel attacks or intrusions that have yet to be experienced. Intrusion detection is the complication of identifying misuse networks [3].The wireless sensor networks consist of tiny sensor nodes which are deployed randomly in various environments. These sensor nodes have limited resources like memory, computational capacity and energy [4]. The function of sensor nodes is to assemble the data and send the collected information to the base station. These sensor nodes are deployed in an hostile and unattended environment, where the nodes are always prone to security attacks. WSN is more susceptible to security breaches due its inherent nature, open environment and unattended hostile environment, limited resources [5]. Among all the other aspects, Security is the most important threat to the networks. The existing security techniques are infeasible due to its limitations like memory, energy and access of nodes after deployment. Subsequently, the security aspect is the most challenging issue that deserves more attention in the wireless sensor networks [7]. Many solutions have been provided to the security issues such as authentication, key exchange, routing protocols etc. They could able to prevent the attacks to some extent and not eliminate the security attacks totally [8]. One of the probable solutions to deal with the security related issues in wireless sensor networks is to make use of the IDS - Intrusion Detection System. It can play a major role in detecting and preventing the attacks [9]. This paper picks to beat the deficiencies of existing arrangements and presents a novel methodology for

 

expanding the BS secrecy. The thought is to frame a progressive directing topology where the BS isn't an evident sink of information activity. Gathering the WSN hubs into groups have been a prevalent plan technique to help versatility, and vitality productivity.

## II. LITERATURE REVIEW

A wireless sensor network (WSN) consists of a set of sensor nodes that are distributed to cover an area of interest and use wireless links to form a connected network topology [10]. These nodes probe the surroundings and transmit their measurements to an in-situ Base-Station (BS). Usually data are routed to the BS over multi-hop paths due to the limited communication range of the individual nodes and to minimize the energy consumption. In addition to the data processing, the BS interfaces the WSN to remote users and gets involved in network management. Such a role makes the BS a critical asset for the WSN and makes a target of security attacks. Basically, in a hostile environment such as a military battlefield, an adversary would favor targeting the BS with attacks to disrupt the WSN operation and nullify its utility to the application [11]. In order to prevent the adversary from distinguishing the BS through the packet header, the identity of the sensor nodes and BS are often concealed by applying anonymous routing techniques [12], [13], [14], [15]. However, the operation model of a WSN makes it possible to determine the location of the BS by intercepting transmissions and employing traffic analysis techniques such as Evidence Theory (ET). Basically, the adversary can eavesdrop and use the received signal strength to determine the position of the source of a transmission and estimate the communication range within which the intended receiver, next hop or the destination, may be located. Considering this as an evidence of the presence of a communication link, the adversary correlates all collected evidences to detect the location of the BS [16], [17], [18].

This paper opts to overcome the shortcomings of existing solutions and presents a novel approach for increasing the BS anonymity. The idea is to form a hierarchical routing topology where the BS is not an apparent sink of data traffic. Grouping the WSN nodes into clusters have been a popular design strategy to support scalability, and energy efficiency [19], [20]. Unlike prior work we devise an anonymity-aware scheme to identify the cluster-heads (CHs) and determine the cluster membership. The clustering criteria also strive to achieve a distribution of CHs that enables the formation of a connected and anonymity-boosting routing topology. A CH receives data packets from the individual sensors in its cluster and generates a single packet of an aggregated packet payload. An anonymity-aware inter-CH routing path is then formed to disseminate the aggregated data to the BS. The route setup is such that it involves CHs that are far from the BS and that only one CH delivers the packets to the BS. Furthermore, the BS selectively transmits the packets to one of the CHs so that it appears as one of the regular network nodes rather than the sink of all traffic. The effectiveness of our approach for forming Hierarchical Anonymity-aware Routing Topology (HART) is validated through simulation and is shown to boost the BS anonymity while incurring nominal overhead [21].

## III. OVERVIEW OF SECURITY PROBLEMS in WSN

WSNs are more vulnerable to security attacks due its open environment. Some of the issues involved in security are listed below [22]:

**Limited Hardware**
The sensor nodes are very tiny and in the recent trends there is requirement to increase the lifetime of the nodes by decreasing the bandwidth consumed, memory etc.Due to this limited resources, establishing security among these nodes is a quite challenging tasks.

**Wireless Communication**
The communication medium is more expensive and it is more susceptible to threats like eavesdropping, inserting malicious nodes into the network, flooding etc.Due to the wireless medium, we can't opt for complicated protocols that require exchange of more information or messages.

**Hostile Environment** Since the sensor nodes are deployed in unattended areas, the hackers can able access the nodes and change the contents. The nodes are not tamper resistant due to its increasing cost which also provides an easy means to the attacker to access the nodes.

**Aggregation Processing**
Sensor nodes generally obtain the information from each sensor and transfer the information to the destination. The lifetime of the sensor nodes can be increased by reducing the communication between the nodes. But this can't be implemented since the sensor nodes have to communicate to perform data processing of sensor nodes.

**Large Scale Deployment**
The present sensor networks use 100s to 1000s of sensors in applications. So scalability is an important factor to be

## IV. INTRUSION DETECTION SYSTEM in WSNs

Security is a major issue in WSN due to its restricted resources like limited resources and vulnerable to physical attacks. Some of the techniques used for security issues include key management, routing protocols, cryptography and security mechanisms for specific attacks and various IDS.The above listed security mechanisms are not sufficient to identify various attacks in WSNs. IDS provide efficient and effective methods to detect the various attacks in WSN. Intrusion detection system is used to detect the intruders in a

 

network. Intrusion is a second line of defense to save the network Intrusion can be defined as an unauthorized activity which is performed in a network. Intrusion detection System tries to collect the data from the network and analyses the data gathered for the abnormal behavior. Intrusion can be achieved collect the data from the network and analyses the data gathered for the abnormal behavior. Intrusion can be achieved in two ways either statically or dynamically. IDS provide much valuable information in the network like the intrusion time; intrusion type; intention of the intruder; position of the intruder; nature of the intruder etc.IDS can only be able to detect the attacks it cannot prevent the attacks. Hence it only used for detecting the attacks [23]. In this paper, various kinds of Intrusion Detection systems are discussed. The components of the IDS are generally classified as: Monitoring Component –Analyze the traffic and keep track of it; Analysis and Detection –Tries to detect the strange behavior in the network; Alarm Component – Once threats identified it raises the alarm [24],[25].

IDS are basically classified into two types based on the audit data: Host based and Network based. Host based depends on the application logs for analyzing the attacks and the network based IDS tries to detect the packets in the network . The IDS can further be classified into various types based on the detection techniques like:

- Anomaly Based IDS
- Signature Based IDS
- Specification Based IDS
- Cross Layer IDS
- Hybrid IDS

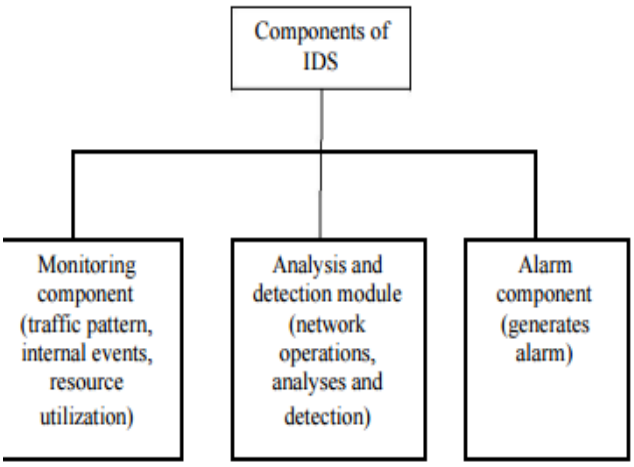


**Figure 1:Components of IDS**

Broadly speaking, IDS has three main components these are defined in figure

***(i) Monitoring component:*** Traffic is monitored using patterns of traffic.

***(ii) Analysis and detection:*** Based on algorithm of modelling behaviour and different activities are analysed and detects the misbehaviour.

***(iii) Alarm component:*** Whenever intrusion is detected alarm is raised by alarm component detection and generation an alarm to report an intrusion has occurred or is in progress. There are two approach of detection intrusion.

**Behavioral Approach:** the observed behavior of the target system is compared to normal and expected behavior. If the behavior of the system is significantly different from the normal or expected behavior, we say that the target system has deficiencies and is subject to an intrusion.

**Scenarios Approach:** In this approach we analyze the audit data in search of attacks predefined scenarios in a database attack signatures. In wireless sensor networks IDSs must satisfy the following properties:

**Local Auditing (Localize auditing):** IDSs for wireless sensor networks work with local and partial audits as in sensor networks wireless data, there is no centralized points that can collect perceivable data auditing.

**Minimum Resources (Minimize resources):** Means that IDSs in sensor network must use a minimum number of resources for networks without son do not have stable connections. More physical resources and network nodes such as power, energy and bandwidth are limited. Disconnection can occur at any time. Communication between nodes for detecting intrusion should therefore not take any available bandwidth.

**No node trust (Trust no node):** IDSs in sensor networks can't trust any node because, unlike wired networks, nodes sensors can be easily compromised.

**Distributed (Be truly distributed):** Means that the collection and analysis of data must be done in different locations. Moreover the distributed approach also applies to the execution of the algorithm of detection and the correlation alerts.

**Safe (Be secure):** intrusion detection system in sensor network should be able to withstand attacks.

**Security Attacks in WSN**

There are many types of attacks possible in WSN. Wireless sensor network are more vulnerable to attacks due to its hostile environment and broadcast nature. The attacks are classified generally as active attacks and passive attacks. Active attacks are dangerous and passive attacks don't modify the data/information and are passive in nature.

 

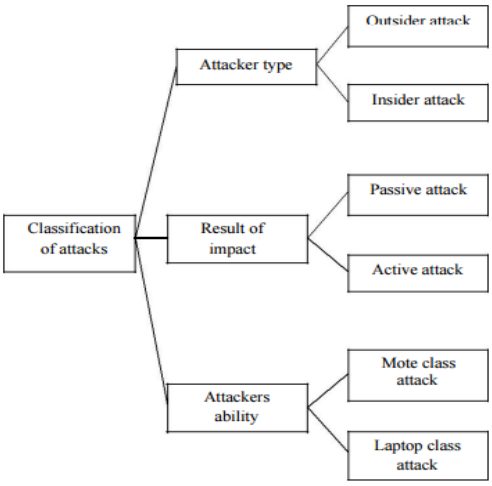


**Figure 2: Attacks in Cloud**

## V. RESEARCH METHODOLOGY

In our work, the comparative study is done based on the basic requirement as Energy efficiency, overhead, and security features include authentication, data confidentiality and integrity. Energy efficiency is the goal is achieved with minimum energy, overhead is due to memory, computation time. By the comparative study, the various methods or architecture for malicious node detection are found. The different techniques are cryptography, ant colony system, trust and reputation. Cryptography is the method of encrypting the message using key, it can be decrypted only the key is know. In the existing works dint fully achieve the security goals, with minimum energy and overhead. And also it does not provide the option for checking whether the reported malicious node is true or not. With this concern, the new algorithm is proposed. The proposed work consists of trust model consists of probability model, HMM model, EAACK based Misbehaviour node verification, and routing through the trusted node. Working of proposed work include

(i) identification of trusted node and
(ii) Routing through the node.

***Proposed Hidden Markov Model***

In this section, we discuss the HMM parameter and their applications to sensor scheduling estimation for WSNs in general. Now we assume that a HMM has N states as $S=(S_1,S_2,...S_N)$, and the state at time t is $q_t$ .The number of distinct observation symbols in each state is M . In general, we denote the observation symbols as $V=(v_1,v_2,...v_M)$ . The state transition probability distribution matrix is denoted as A , where A denotes as follows:

$$A=[a_{ij}],\sum_{j=1}^{N}a_{ij}=1$$

$$a_{ij}=P[q_{i+1}=S_j\,|\,q_t=S_i],i,j\in[1,N]$$

We denote the probability of observation as $B=[b_j(k)]$, where $b_j(k)=P[v_k\,|\,q_t=S_j]$. If there are M possible observation matrix B is composed of $b_j(k)$ with M rows and N columns, moreover $\sum_{k=1}^{M}b_j(k)=1$ . In the practical application, we can initial state distribution probability. What is the probability the first state $q_1\in S$ in HMM system.

***Proposed Approach for Identification of Trusted Node***

We can find the trust node based on probability model and HMM (Message Authentication Code) mode

l. Probability model gives trust value based on behaviour of node. In HMM model the verification of HMM is done.

2. If the HMM does not match, it goes to secure Acknowledgement mode. The report is sent to source and verifies the reported node by using misbehaving report phase.

***Routing through the node***

Once the trusted node is found the BFS algorithm is implemented in this.

The working procedure is of the proposed work is explained below

**Step1:**

Select the Probability model:

ii.Assume an threshold value as 0.5,

iii. The nodes are given a rating based on the nodes behaviour.

iv. If rating above 0.5, considered as trusted node v. Otherwise it is un trusted.

***Step2:***

Select the HMM model

i. In this the message are encrypted by using the key, and it is send to the trusted nodes. The message is recomputed and HMM is checked.

ii. Mobile agents are responsible for carrying the encrypted message to check the HMM verification.

iii. If it is matches considered as trusted node and send Ack to the source.

iv. Otherwise move to step3

***Step3:***

Secure Acknowledgement (ACK) phase

i. In secure acknowledgement (S-ACK) phase three nodes work together to find the malicious node, the node R4 sends S-ACK data packet (pkt1) to R5, then R5 forwards this packet to i6.the node R6 receives the pkt1 it has to send the S-ACK packet to R4.

iii. If R4 does not receive this acknowledgement, then the node R4 is considered to be malicious. It is reported to the source node.

 

iv. The source node switches to the Misbehaviour Report Authentication (MRA) mode to ensure that the node is malicious or not

***Step4:***

Misbehaviour (malicious) report phase

i. In MRA mode, it checks whether the reported malicious node is true or not.

ii. It checks whether the missing packet is reached the destination through any other node. When the destination node receives the MRA packet, it checks its local knowledgebase.

iii. If the missed packet is already received by destination node through different path. It is concluded that it is a false misbehaviour report. That is R4 is considered as a malicious node is not true, who generated the report that is R6 is considered as malicious node.

iv. Otherwise the misbehaviour report is considered as true. The static agents and mobile agents are implanted in each node static agents triggers the mobile agent to collect the information about the trusted node and malicious node and its path towards the destination

## VI. RESULTS AND DISCUSSIONS

The functionality of wireless network is based on the performance of efficiency, loss and successful transmission rate of packet in the network. In this paper, proposed a effective IDS - HMM approach for effective transmission of data packet in the multi-rate wireless network. In the multi - rate scenario SINR is the major constraint for effective transmission and reception of data packet. To avoid congestion in channel this research uses IDS - HMM generates random key generation with integral hashing with elliptical curve approach. The proposed approach minimizes payload in data transmission in channel with appropriate number of bits. Proposed IDS - HMM approach simulation performance is based on NS2 simulation software. Simulated results observed for proposed IDS - HMM is comparatively analyzed and presented in this section. The simulation performance of proposed approach is comparatively examined with other existing approaches like ARF with COLLIE (AC), Adaptation of Link Rate and Contention Window (ARC), Receiver-based Auto-rate (RBAR) and Enhanced Adaptation of link Rate and Contention window (EARC)

We have used NS2 (Network Simulator 2) for simulation. NS is an Object-oriented Tcl(Otcl) script interpreter that has a simulation event scheduler and network component object libraries, and network set-up module libraries. The simulated results show the malicious node identification in the network. In this the simulated model designed as such the source node receives the signal it performs the process and identifies the trusted and malicious nodes and routing is done that is the data packet is transferred. And the performance metrics are analyzed by using graph. In this the simulated graph results are analyzed. The existing system, is compared with our proposed work. The main factors include energy consumption, memory overhead and packet delivery ratio.

**Energy Consumption**

Energy consumption is the usage of battery source. Energy overhead of monitoring involves− (i) the energy spent by the CPU for running algorithm (ii) the energy spent in sending/receiving packets related to monitoring such as neighbor discovery and malicious node detection announcements. The power is used to transmit and receive the packets. It is an flooding based technique, it does not retransmit any packets.

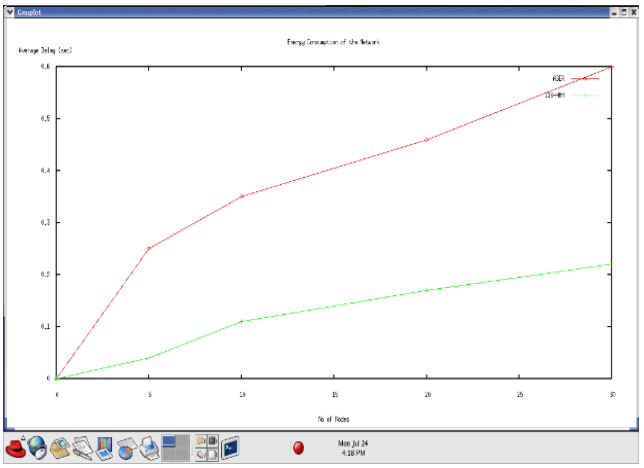

Figure 3 Energy consumption

The figure demonstrates the performance comparison plot for the routing overhead in the multi - rate wireless network for proposed approach. Through the simulation graph it is clearly observed that proposed IDS - HMM provide effective routing overhead than other existing algorithm. Also it is identified that HMM algorithm also provides almost similar characteristics as of IDS - HMM algorithm. Other approaches AC, RBAR and ARC routing values are significantly higher than the proposed approach. As the time increases routing overhead also increases in the IDS - HMM and for time 90 the value is obtained as 28 which is significantly minimal than other approaches.

**Memory Overhead**

Memory overhead is the amount of memory it requires to store the values that is need for the process of finding malicious node.

 

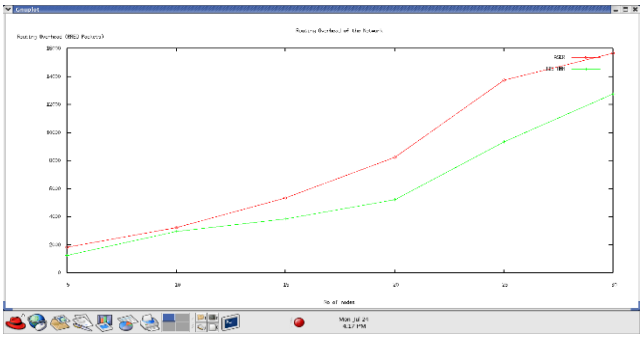

Figure 4 Memory Overhead

Routing overhead is critical scenario in wireless network system by small sized packet entire network aware of characteristics of network. Through the available information in wireless network channel routes the packet for transmission of data in the network with effective utilization of available bandwidth.

The figure demonstrates the performance comparison plot for the routing overhead in the multi - rate wireless network for proposed approach. Through the simulation graph it is clearly observed that proposed IDS - HMM provide effective routing overhead than other existing algorithm. Also it is identified that HMM algorithm also provides almost similar characteristics as of IDS - HMM algorithm. Other approaches AC, RBAR and ARC routing values are significantly higher than the proposed approach. As the time increases routing overhead also increases in the IDS - HMM and for time 90 the value is obtained as 28 which is significantly minimal than other approaches.

**Packet Delivery Ratio (PDR)**

PDR is defined as the number of data packets transmitted to the data packet received at the destination. The malicious nodes are identified accurately, the possibility of packets drop is minimum.

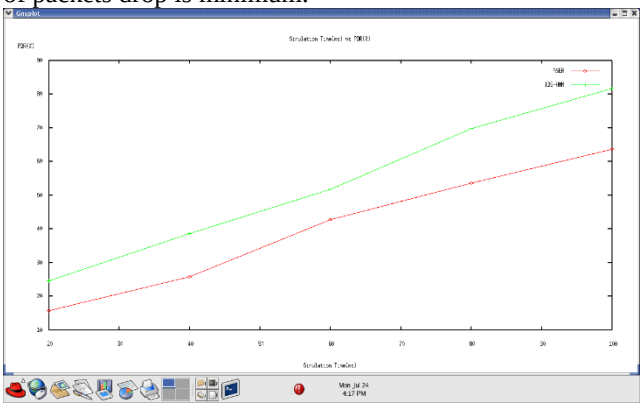

Figure 5 Packet Delivery Ratio

PDR is the contrast factor for PLR, in PDR number of packets received in the receiver end is evaluated with respect to the number of transmitted packet. Effective wireless network need to have significant PDR value for effective performance in the network. PDR for proposed IDS - HMM is maximal than other technique in IEEE 802.11 network. Maximum PDR value for proposed approach is 0.98. Here EARC algorithm provides almost similar characteristics as of IDS - HMM whose PDR value is 0.96. Whereas AC, ARC and RBAR values are 0.4, 0.47 and 0.58 respectively.

**Delay**

The delay of a network specifies how long it takes for the data to travel across the network from source node to destination. The time required to compute the MAC model, finding the malicious nodes also determines the delay of the network.

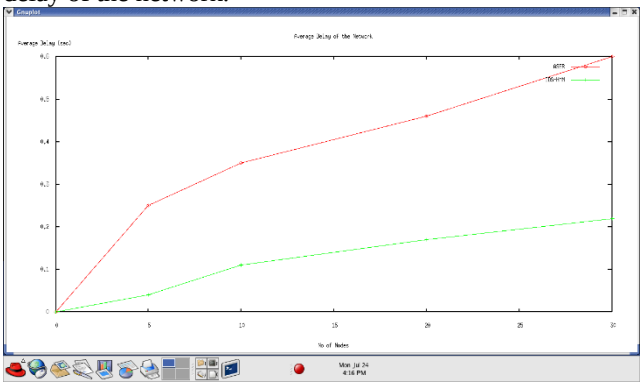

Figure 6 Delay performances in the network

All the above figures red line indicates existing system and green line indicates proposed system. Overall delay is defined as time taken by the packet to reach between sender to receiver in wireless network. Similar to other characteristics performance overall delay also minimal for proposed IDS - HMM techniques. The maximum delay obtained for wireless network of proposed approach is 30 minimal than other techniques.

**Table 1 Proposed system performance**

| Parameters | Proposed Method |
|---|---|
| packet delay | 14ms |
| Average number of Hops | 3 hop nodes |
| Execution time | 100 ms |
| Energy consumption | 21% |
| Energy Efficiency | 79% |
| End to End Delay | 0.229 % |
| Dropped Reply Messages | 9 pacs |
| packet delivery ratio | 89% |
| Throughput | 198 kbps |

The table1 provides comparative performance analysis of proposed approach with respect to performance in the

 

Intrusion Detection System. Comparative analysis of table also illustrated that proposed IDS - HMM scheme perform effectively interms of packet delay, execution time, number of hops values of 14ms, 100ms and 3 hop nodes respectively. The evaluation of other parameters for wireless sensor network also provides Energy consumption value of 21% and end-to-end delay of 0.229%. Even proposed IDS - HMM scheme exhibits effective performance in terms of throughput, delay and dropped messages count.

## VII. CONCLUSION

WSN are deployed in hostile environment and because of its wireless nature it is subjected to various kinds of attacks, information loss and modification. It is important in WSN the sensed data packets should reach the destination within the particular time and also the data packets should not undergo any modification. In our work, The trusted nodes are identified by the HMM model and it is rated. HMM model effectively identifies the un trusted node by using SHA algorithm. The data packets are routed through the trusted node. Trusted node gives security features such as confidentiality, integrity and authentication because it is identified by HMM model. The nodes are rated which is based on data transfer and friendship with other nodes, this provides complete information of the node. And also the un trusted nodes are given a chance to prove it is really malicious or not. The trusted nodes are identified effectively. The nodes are free from attacks.

## REFERENCES


[1]. Chong, C. Y., & Kumar, S. P. (2003). Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE, 91(8), 1247-1256.

[2]. Perrig, A., Stankovic, J., & Wagner, D. (2004). security in wireless sensor networks" communications of the ACM, vol. 47, no. 6.

[3]. Mourabit, Y. E., Toumanari, A., Bouirden, A., Zougagh, H., & Latif, R. (2014, November). Intrusion detection system in Wireless Sensor Network based on mobile agent. In Complex Systems (WCCS), 2014 Second World Conference on (pp. 248-251). IEEE.

[4]. Ning, P., Cui, Y., & Reeves, D. S. (2002, November). Constructing attack scenarios through correlation of intrusion alerts. In Proceedings of the 9th ACM Conference on Computer and Communications Security (pp. 245-254). ACM.

[5]. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks.

[6]. Shanthi, S., & Rajan, E. G. (2016, October). Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks. In Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on (pp. 426-431). IEEE.

[7]. 7. Panigrahi, R., Sharma, K., & Ghose, M. K. (2013). Wireless Sensor Networks–Architecture, Security Requirements, Security Threats and its Countermeasures. CS & IT-CSCP, AIRCC Publishing Corporation.

[8]. 8. Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[9]. 9. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks.

[10]. 10 . Karl, H., & Willig, A. (2007). Protocols and architectures for wireless sensor networks. John Wiley & Sons.

[11]. 11. Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. computer, 35(10), 54-62.

[12]. 12. Zhang, Y., Liu, W., & Lou, W. (2005, March). Anonymous communications in mobile ad hoc networks. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (Vol. 3, pp. 1940-1951). IEEE.

[13]. 13. Boukerche, A., El-Khatib, K., Xu, L., & Korba, L. (2004, October). A novel solution for achieving anonymity in wireless ad hoc networks. In Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (pp. 30-38). ACM.

[14]. 14. Jiang, J. R., Sheu, J. P., Tu, C., & Wu, J. W. (2011). An Anonymous Path Routing (APR) Protocol for Wireless Sensor Networks. J. Inf. Sci. Eng., 27(2), 657-680.

[15]. 15. Chen, C. W., & Tsai, Y. R. (2011). Location privacy in unattended wireless sensor networks upon the requirement of data survivability. IEEE Journal on Selected Areas in Communications, 29(7), 1480-1490.

[16]. 16. Acharya, U., & Younis, M. (2010). Increasing base-station anonymity in wireless sensor networks. Ad Hoc Networks, 8(8), 791-809.

[17]. 17. Huang, D. (2006, November). On measuring anonymity for wireless mobile ad-hoc networks. In Local Computer Networks, Proceedings 2006 31st IEEE Conference on (pp. 779-786). IEEE.

[18]. 18. Mehta, K., Liu, D., & Wright, M. (2012). Protecting location privacy in sensor networks against a global eavesdropper. IEEE Transactions on Mobile Computing, 11(2), 320-336.

[19]. 19. Abbasi, A. A., & Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. Computer communications, 30(14), 2826-2841.

[20]. 20. Afsar, M. M., & Tayarani-N, M. H. (2014). Clustering in sensor networks: A literature survey. Journal of Network and Computer Applications, 46, 198-226.

[21]. 21. Alsemairi, S., & Younis, M. (2015, December). Clustering-Based Mitigation of Anonymity Attacks in Wireless Sensor Networks. In Global Communications Conference (GLOBECOM), 2015 IEEE (pp. 1-7). IEEE.

[22]. 22. Panigrahi, R., Sharma, K., & Ghose, M. K. (2013). Wireless Sensor Networks–Architecture, Security Requirements, Security Threats and its Countermeasures. CS & IT-CSCP, AIRCC Publishing Corporation.

[23]. 23. Duhan, S., & Khandnor, P. (2016, March). Intrusion detection system in wireless sensor networks: A comprehensive review. In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on (pp. 2707-2713). IEEE.

[24]. 24. Krontiris, I., Dimitriou, T., Giannetsos, T., & Mpasoukos, M. (2007, July). Intrusion detection of sinkhole attacks in wireless sensor networks. In International Symposium on Algorithms and Experiments for Sensor Systems, Wireless


 

Networks and Distributed Robotics (pp. 150-161). Springer Berlin Heidelberg.
[25]. 25. Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: a review. International Journal of Distributed Sensor Networks.
[26]. 26. Anagha S. Anand, V. S. Anitha Implementation and Analysis of k-Barrier Coverage in Wireless Sensor Networks. International Journal of Computer Sciences and Engineering Vol-6, Special Issue-6, July 2018.
[27]. 27. H. Kaur , K. Kaur Review Paper on Cryptography Algorithms Used in Wireless Sensor Networks. International Journal of Computer Sciences and Engineering Vol-6, Issue-8, Aug 2018.

**Author Profile**

Dr.S. Jawahar received his MCA. Degree from Bharathidasan University, Trichy, India in 1998. He also received his Ph.D degree in University of Madras, India in 2016. Now he is working as a Associate Professor and Head, Department of MCA, Asan Memorial College, Chennai, India. His research area is Neural Network and Data Structure.

Dr.J. Adamkani received his M.Sc., degree From University of Madras, Chennai, India in 2003. He also received his Ph.D. degree in University of Madras, India in 2017. Now he is working as a Assistant Professor with Department of Computer Science, The New College, Chennai, India. His research area is Data Mining and Network Security.

 