IJRSET NOVEMBER 2017 Volume 4, Issue 11 Pages: 33-40

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

ANALYSIS AND SURVEY ON WIRELESS SENSOR NETWORK BASED SECURITY IDS

[1] S. MURALI, [2] Dr. V. SATHYA,
[1, 2] Assistant Professor,
[1, 2] MGR College, Hosur,
[1, 2] Tamil Nadu, India.

ABSTRACT - Wireless Sensor Networking is one of the most encouraging technologies that have applications going from social insurance to tactical military. Albeit Wireless Sensor Networks (WSNs) have engaging highlights (e.g., low installation cost, unattended network operation), because of the lack of a physical line of resistance (i.e., there are no entryways or switches to monitor the information flow), the security of such networks is a major concern, especially for the applications where confidentiality has prime importance. Intrusion detection is a constant monitoring and analysis of network activity and data for potential Vulnerabilities and attacks in advancement. In this paper Digital Signature Algorithm (DSA), RSA algorithms are broke down.

Keywords: [Digital Signature Algorithm, RSA algorithm, Wireless Sensor Networks, Security.]

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are disseminated, infrastructure less, shortcoming tolerant, scalable and dynamic in nature. These networks are minimal effort and simple to introduce in a zone. These are based upon little measured, low power and self-controlled hubs called sensor hubs. These hubs have little memory, less computation capacity and short lifetime (relies upon battery life). Sensor hubs assemble helpful information from their environment and transmit it to the client controlled system called Base Station (BS) or sink for analysis. Such networks may be utilized for war zone surveillance, making a decision about volcanic conduct, peering toward creature development, predicting torrent, etc. Sensor hubs are thickly conveyed in the sensor field (zone under consideration). They keep up a topology and start sensing the environment. Their topology is dynamic and changes every now and again attributable to the limitations of the sensor hubs. Sensor hubs may get harmed inferable from substantial breeze, downpour, daylight, creatures, etc., or their battery may deplete. Here, routing protocol assumes a significant job because hubs leave or join the sensor network at sporadic interims.

Security is a noteworthy concern for a wide range of network paradigms whether they are wired networks, mobile ad hoc networks or recently rising IP Multimedia Subsystems (IMSs). WSNs are powerless against a few kinds of security dangers that can degrade the general performance of these networks. Security attacks against WSNs are categorized into two primary branches: Active and

Passive. In detached attacks, at-tackers are typically camouflaged (covered up) and either tap the communication link to collect data; or devastate the functioning components of the network. Uninvolved attacks can be assembled into listening stealthily, hub malfunctioning, hub altering/destruction and traffic analysis types. In active attacks, an enemy really influences the activities in the attacked network. This impact may be the target of the attack and can be detected. For instance, the networking services might be degraded or ended because of these attacks. Active attacks can be assembled into Denial-of-Service (DoS), sticking, opening attacks (blackhole, wormhole, sinkhole, etc.), flooding and Sybil types. Readers who are intrigued more on security attacks against WSNs.

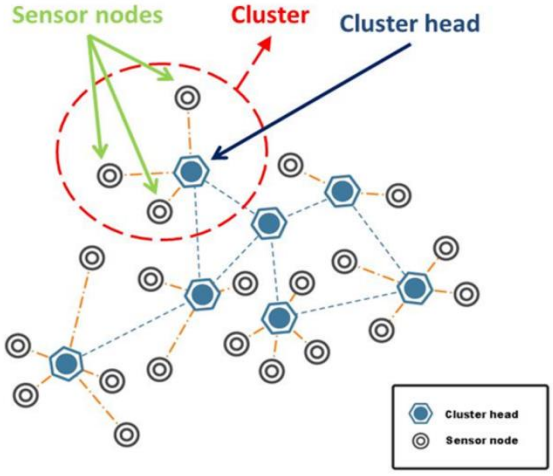

Figure 1: Wireless Sensor Network based security on IDS.

In any security plan, Intrusion Detection Systems (IDSs) give a few or the majority of the accompanying information to the next supportive systems: identification of the interloper, location of the gatecrasher (e.g., single hub or regional), time (e.g., date) of the intrusion, intrusion activity (e.g., active or aloof), intrusion type (e.g., attacks such as worm gap, black gap, sink opening, selective sending, etc.), layer where the intrusion occurs (e.g., physical, data link, network). This information would be exceptionally useful in moderating (i.e., third line of barrier) and curing the consequence of attacks, since very specific infor-mation with respect to the interloper is acquired. In this manner, intrusion detection systems are significant for network security.

2. LITERATURE SURVEY

Faiza Medjek, , Djamel Tandjaoui, Imed Romdhani, Nabil Djedjig (2017) Proposed a trust-based intrusion detection system for mobile RPL based networks. Another timer and minor extensions to RPL messages arrangement to manage portability, character and multicast issues. In addition, each hub is equipped with a Trusted Platform Module co-processor to handle identification and off-load security related computation and capacity. In T-IDS, each hub is considered as monitoring hub and collaborates with his friends to detect intrusions and report them to a 6LoWPAN Border Router (6BR). The IDS is hierarchical where three layer cooperate to handle attacks: the Backbone Router, the 6LoWPAN Border Router, and the in-network hubs. Besides, T-IDS utilizes three modules: IdentityMod, MobilityMod, and IDSMod to detect and dodge malicious hubs. Regardless of whether T-IDS is by all accounts resources costly, to accept that off-loading security computations and data-stockpiling utilizing TPM reduces the cost. **Safa Otoum, Burak Kantarci, Hussein T. Mouftah (2017)** Proposed an alleviating false negative gatecrasher decisions in wsn-based brilliant lattice monitoring. Clustered Hierarchal Hybrid-Intrusion Detection System (CHH-IDS) that is in charge of various attacks infused by known and obscure gatecrashers. As False Positives (FPs) and False Negatives (FNs) are the key performance parameters in IDS, to examine mitigation of FNs through a two-level intrusion detection approach, which manages abnormality and signature detection in parallel. The False Negative (FN) performance of a hybrid intrusion detection system which utilizes an inconsistency detection subsystem for unknown attacks and signature detection subsystem for known attacks to SG infrastructure that is monitored

through a WSN. The False Negative Ratios (FNR) can be significantly reduced as unknown attacks structure most of the attack population. Random Forest is expected to have higher detection ratios, it is beyond the realm of imagination to expect to direct 100% of the data to the irregularity detection subsystem. **Salavat Marian, Popa Mircea (2015)** Proposed a sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme. In the present current wireless sensor networks, there are two known indicators for link quality estimation: Received Signal Strength Indicator and Link Quality Indicator (LQI). RSSI in ZigBee protocols is steady enough so as to utilize it in a security mechanism. lightweight - detection mechanism for Sybil attacks based on three hub collaboration utilizing only their received signal strength indicator with no different computations or piggybacking message sending. To achieve a lightweight detection solution, must reduce computation inside the hub as less as could reasonably be expected. In ZigBee protocol, the RSSI worth is equipment based and is transmitted as a matter of course without the need of piggybacking the packets with additional data. By utilizing the RSSI proportion of three receivers, to compute the location of a sender and in this way classify it as a gatecrasher or as a "good" hub. **Jafar Abo Nada, Mohammad Rasmi Al-Mosa (2018)** Proposed a wireless intrusion detection prevention and attack system. The improvement of an intrusion detection system on wireless networks which is Wireless Intrusion Detection Prevention and Attack System "WIDPAS". It is based on three primary tasks: monitoring, analysis and protection. Through which it monitors denial of service attacks or false networks and then investigates the attack and recognizes the attacker and then protects the network clients. Wireless intrusion detection accessible solution system in the markets, including commercial or free open source, and applies the vast majority of the functions of detection and decide the sort of attack. To increase the effectiveness of the system in the work environment where the system can monitor the greater part of the attacks and the system can Defend the network from counterfeit networks by attacking the attacker and cut the way towards the attacker and protect the staff from being scammed. **Rubal Grewal, Kamaljit Singh Saini (2015)** Proposed a protection mechanism against clone wars in hierarchical based wireless sensor networks. propose a mechanism based on the utilization of hub ID and location information to detect replicated hubs by the base station in hierarchical based networks. The scheme is based on the centralized approach. the scheme achieves most extreme detection probability with low communication overhead as compared to Line selected Multicast protocol. Another scheme is proposed to detect replication attack based on three-level hierarchical architecture of WSNs. The scheme is based on the utilization of location information and personality of each hub which is collected by each cluster head from the cluster part hubs. Each cluster head transmits the information to the BS that detects the presence of replicated hubs in the network. **Tsítso Maphatsoe, Muthoni Masinde (2018)** proposed asymptotic analysis of a fuzzy based intrusion detection system for zigbee. To applying asymptotic analysis to assess the performance of a peculiarity detection algorithm which is designed utilizing logic reasoning through fuzzy logic approachs. So as to achieve this, the IDS was included as a component of intrusion detection software for ZigBee Wireless Sensor Networks (WSNs). An IDS system that makes utilization of a fuzzy logic installed security algorithm, to monitor for dangers in a ZigBee WSN by conglomerating, making calculations and assumptions based on the information received from the hubs the minute they send in data from monitoring assignments. Besides, before its implementation, the performance of the algorithm was decide utilizing asymptotic analysis where the Big OH was resolved. This

empowered the determination how well it admissions as the quantity of hubs in a network unavoidable detonate in size. The asymptotic calculations indicated that the algorithm will execute in direct time as the size of the network develops. This is a decent

3. WSN BASED SECURITY IDS ALGORITHMS

3.1. DIGITAL SIGNATURE ALGORITHM

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures, based on the mathematical concept of particular exponentiation and the discrete logarithm issue. DSA is a variation of the Schnorr and ElGamal signature schemes. The Digital Signature Algorithm (DSA) can be utilized by the recipient of a message to check that the message has not been adjusted during travel just as ascertain the originator's personality. A digital signature is an electronic version of a composed signature in that the digital signature can be utilized in demonstrating to the recipient or an outsider that the message was, in fact, marked by the originator. Digital signatures may moreover be produced for set away data and tasks with the objective that the decency of the information and activities may be checked at any later time.The DSA is used by a signatory to create a digital signature on data and by a verifier to affirm the authenticity of the signature. Each signatory has a public and private key. The private key is utilized in the signature generation process and the public key is utilized in the signature verification process. For both signature generation and check, the information (which is implied as a message) is diminished by methods for the Secure Hash Algorithm (SHA) determined in FIPS 180-1. An enemy, who doesn't have the foggiest thought regarding the private key of the signatory, can't create the right signature of the signatory. As it were, signatures cannot be fashioned. In any case, by utilizing the signatory's public key, anyone can check a correctly marked message.

A Digital Signature Scheme will have two components, a private marking algorithm which allows a client to securely sign a message and a public verification algorithm which licenses anyone to confirm that the signature is authentic. The marking algorithm needs to "tie" a signature to a message in such a manner that the signature can not be destroyed out and used to sign another document, or have the first message adjusted and the signature stay substantial. For practical reasons it would be necessary for the two algorithms to be generally quick and if little computers such as savvy cards are to be utilized. There are numerous Digital Signature Schemes which meet these conditions, yet we will only research a couple of the most prevalent ones.

3.2. RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two distinctive keys for example Public Key and Private Key. The RSA cryptography algorithm is the most generally utilized public key cryphotography algorithm on the planet. It tends to be to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be utilized for both public key encryption and digital signatures. Its security is based on the difficulty of factoring huge numbers. Cryptographic strategies cannot be demonstrated secure. Instead, the only test is to check whether someone can make sense of how to decipher a message without having direct knowledge of the decryption key. The RSA technique's security lays on the fact that it is incredibly difficult to factor enormous numbers. On the off chance that 100 digit numbers are utilized for p and q, the subsequent n will be around 200 digits.

Encryption is the act of encoding content with the goal that others not aware of the decryption mechanism (the "key") cannot understand the content of the content. Encryption has long been the area of covert operatives and diplomats, yet recently it has

moved into the public eye with the concern of the protection of electronic transmissions and digitally put away data. Standard encryption strategies for the most part have two basic imperfections: (1) A secure channel must be built up sooner or later so the sender may exchange the decoding key with the receiver; and (2) There is no assurance who sent a given message. Public key encryption has quickly developed in fame (and controversy, see, for instance, discussions of the Clipper chip on the archives given underneath) because it offers a secure encryption technique that addresses these concerns. In a classic cryptosystem so as to make sure that no one, except the planned recipient, deciphers the message, the individuals included had to endeavor to keep the key secret.

4. APPLICATIONS OF WSN BASED SECURITY IDS

- Military or Border Surveillance Applications WSNs are becoming a fundamental piece of military command, control, communication and intelligence systems. Sensors can be conveyed in a war zone to monitor the presence of forces and vehicles, and track their developments, empowering close surveillance of contradicting forces.
- Environmental Applications Environmental applications include tracking the developments and patterns of insects, feathered creatures or little creatures.
- Health Care Applications Wireless sensor networks can be utilized to monitor and track seniors and patients for social insurance purposes, which can significantly alleviate the extreme deficiency of human services personnel and reduce the medicinal services consumptions in the current social insurance systems. For instance sensors can be conveyed in a patient's home to monitor the practices of the patient. It can caution doctors when the patient falls and requires prompt medical attention.
- Environmental Conditions Monitoring WSN applications around there incorporate monitoring the ecological conditions influencing yields or domesticated animals, monitoring temperature, stickiness and lighting in office structures, etc. These monitoring modules could even be joined with actuator modules which can control, for example , the proportion of manure in the dirt, or the proportion of cooling or warming in a structure, in view of flowed sensor estimations.
- Home Intelligence Wireless sensor networks can be utilized to give increasingly convenient and smart living environments for individuals. For example, wireless sensors can be used to remotely peruse utility meters in a home like water, gas, power and after that send the readings to a remote focus through wireless correspondence.
- Industrial Process Control In industry, WSNs can be used to screen assembling process or the state of assembling hardware. These sensors are utilized to alarm in case of any disappointments occurred.
- Agriculture Using wireless sensor networks inside the agricultural business is increasingly common; utilizing a wireless network liberates the rancher. Irrigation automation empowers progressively efficient water use and reduces squander.
- Structural Monitoring Wireless sensors can be utilized to monitor the development inside structures and infrastructure such as scaffolds, flyovers, embankments, burrows etc... empowering Engineering practices to monitor resources remotely without the requirement for costly site visits, just as having the advantage of day by day data, though traditionally this data was collected weekly or monthly, utilizing physical site visits, including either road or rail closure sometimes. It is likewise unquestionably more accurate than any visual inspection that would be carried out.

5. Experimental Results

Traffic Ratio

Digital Signature Algorithm	RSA Algorithm
76	52
77.4	57
79.1	66
79.5	70
90.1	80.6

Table 1: Comparison table of Traffic Ratio

The comparison table of Traffic ratio of Digital Signature Algorithm and RSA Algorithm shows the different values. While comparing the Digital Signature Algorithm and RSA Algorithm the RSA algorithm values is better than the Digital Signature Algorithm. The Digital Signature Algorithm value starts from 76 to 90.1 and the RSA algorithm values starts from 52 to 80.6. Every time the RSA algorithm gives the better results.

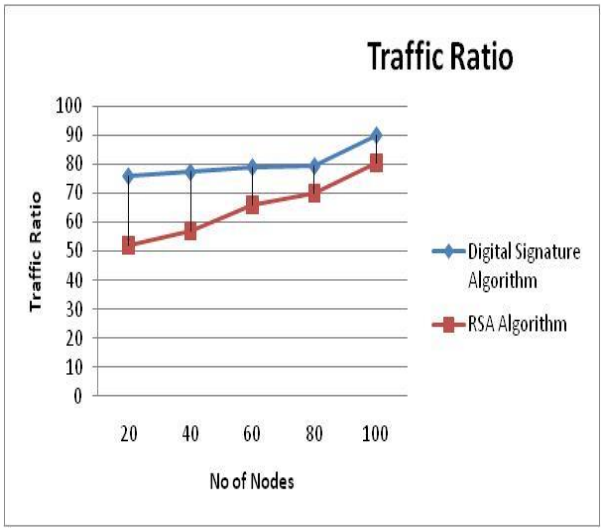

Figure 2: Comparison Chart of Traffic Ratio

The comparison chart of Traffic Ratio of Digital Signature Algorithm and RSA Algorithm demonstrates the different values. No of nodes in x axis and Traffic ratio in y axis. The RSA algorithm is better than the Digital Signature Algorithm. The Digital Signature Algorithm value starts from 76 to 90.1 and the RSA algorithm values starts from 52 to 80.6. Every time the RSA algorithm gives the better results.

THROUGHPUT RATIO

Digital Signature Algorithm	RSA Algorithm
50	83.6
55	85.6
60	87.6
65	89.1
70	93.9

Table 2: Comparison table of Throughput Ratio

The comparison table of Throughput ratio of Digital Signature Algorithm and RSA Algorithm shows the different values. While comparing the Digital Signature Algorithm and RSA Algorithm the RSA algorithm is better than the Digital Signature Algorithm. The Digital Signature Algorithm value starts from 50 to 70 and the RSA algorithm values starts from 83.6 to 93.9. Every time the RSA algorithm gives the great results.

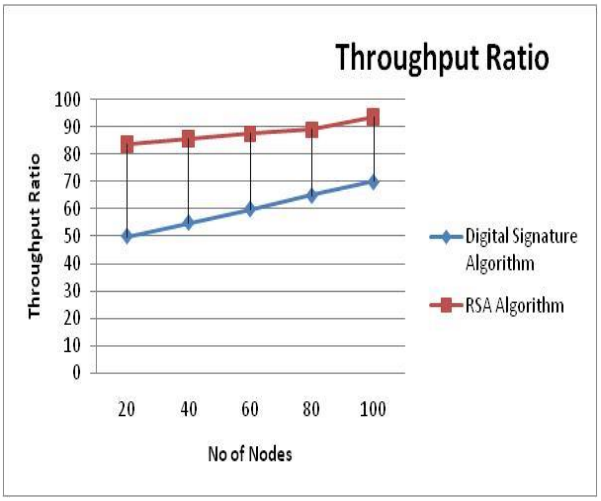

Figure 3: Comparison Chart of Throughput Ratio

The comparison chart of throughput Ratio of Digital Signature Algorithm and RSA Algorithm demonstrates the different values. No of nodes in x axis and Throughput ratio in

y axis. The RSA algorithm is better than the Digital Signature Algorithm. The Digital Signature Algorithm value starts from 50 to 70 and the RSA algorithm values starts from 83.6 to 93.9. Every time the RSA algorithm gives the great results.

EFFECTIVE RATIO

Digital Signature Algorithm	RSA Algorithm
69.5	73.6
69.9	75.6
69.5	77.6
70.8	78.6
71.9	79.8

Table 3: Comparison table of Effective Ratio

The comparison table of Effective ratio of Digital Signature Algorithm and RSA Algorithm shows the different values. While comparing the Digital Signature Algorithm and RSA Algorithm the RSA algorithm is better than the Digital Signature Algorithm. The Digital Signature Algorithm value starts from 69.5 to 71.9 and the RSA algorithm values starts from 73.6 to 79.8. Every time the RSA algorithm gives the great results.

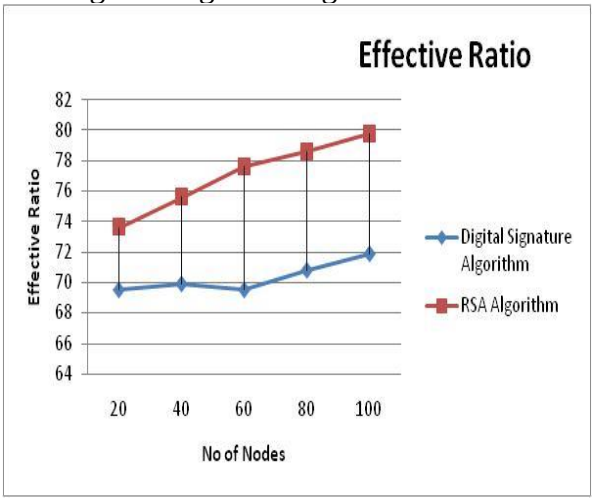

Figure 4: Comparison Chart of Effective Ratio

The comparison chart of Effective Ratio of Digital Signature Algorithm and RSA Algorithm demonstrates the different values. No of nodes in x axis and Effective ratio in y axis. The RSA algorithm is better than the Digital Signature Algorithm. The Digital Signature Algorithm value starts from 69.5 to 71.9 and the RSA algorithm values starts from 73.6 to 79.8. Every time the RSA algorithm gives the great results.

CONCLUSION

The key challenge of advancing intrusion detection system in WSN is to recognize attacks with high accuracy, and fulfilled the required constraints. As the WSN becomes necessary and utilized much of the time for some applications, the requirement for securing them is likewise increasing because of the idea of their sending and their resource restrictions. Cryptographic and authentication protocols have been proposed to protect these networks from untouchable intrusions however neglect to protect them from the insider ones. In this paper there are various algorithms to execute Wireless Sensor Network in security Intrusion Detection System (IDS).These various algorithms for Intrusion Detection System (IDS) Algorithm, Digital Signature Algorithm, RSA Algorithms are discussed and some are compared based on their performance.

REFERENCES

[1]. Faiza Medjek, , Djamel Tandjaoui, Imed Romdhani, Nabil Djedjig," A Trust-based Intrusion Detection System for Mobile RPL Based Networks", 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)

[2]. Safa Otoum, Burak Kantarci, Hussein T. Mouftah," Mitigating False Negative Intruder Decisions in WSN-based Smart Grid Monitoring", ©2017 IEEE

[3]. Salavat Marian, Popa Mircea," Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator detection scheme", ©2015 IEEE

[4]. Jafar Abo Nada, Mohammad Rasmi Al-Mosa," A Proposed Wireless Intrusion Detection Prevention and Attack System", ©2018 IEEE
[5]. Rubal Grewal, Kamaljit Singh Saini," A Defense Mechanism Against Clone Wars in Hierarchical Based Wireless Sensor Networks", ©2015 IEEE.
[6]. Tsítso Maphatsoe, Muthoni Masinde," Asymptotic Analysis of A Fuzzy Based Intrusion Detection System For Zigbee", ©2018 IEEE
[7]. Jin Xu, Xu Wu and Xiaqing Xie," Efficient Identity-Based Offline/Online Encryption Scheme for Lightweight Devices", 2018 IEEE Third International Conference on Data Science in Cyberspace.
[8]. Ms. Shelke Shailaja, Ashwini B. Patil," Energy Efficient Intrusion Detection Scheme Based on Bayesian Energy Prediction in WSN", © 2015 IEEE
[9]. Raghu Vamsi and Krishna Kant," Secure Data Aggregation and Intrusion Detection in Wireless Sensor Networks", ©2015 IEEE
[10]. Yu Zeng, Xing Zhang, Rizwan Akhtar, Changda Wang," A Blockchain-Based Scheme for Secure Data Provenance in Wireless Sensor Networks", ©2018 IEEE
[11]. Roshani R. Patle, Rachana Satao," Aggregated Identity-Based Signature To Transmit Data Securely and Efficiently in Clustered WSNs", © 2015 IEEE
[12]. Aswathy Balakrishnan, Rino PC," A novel anomaly detection algorithm for WSN", © 2015 IEEE
[13]. Amar Amouri, Vishwa T. Alaparthy and Salvatore D. Morgera," Cross layer-based intrusion detection based on network behavior for IoT", ©2018 IEEE
[14]. Jitendra Singh, Vimal Kumar, Rakesh Kumar," An RSA Based Certificateless Signature Scheme for Wireless Sensor Networks", ©20 15 IEEE
[15]. Chaitali Biswas Dutta, Utpal Biswas," Intrusion Detection System for Power-Aware OLSR, © 2015 IEEE