IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205508 |

A Study on Secure Data Transmission in Wireless Sensor Networks

Dr. H K Shankarananda

HOD, Department of E&C, TMAES Polytechnic (Govt Aided), Hosapete, India

ABSTRACT: A productive approach is to integrate security awareness into the network-layer delivery mechanisms, such as multichip routing or longer-range physical layer approaches. An ideal approach would be workable within realistic channel conditions, impose no complexity for additional control packets or sentry packets, while being fully distributed and scalable. This study leverages Enhanced Adaptive Acknowledgment, which checks for the existence of hostile nodes before rule sharing, to enable secure rule sharing. This would take place during intraregional leaders' rule-sharing sessions. To optimize memory storage and address bandwidths/memory concerns, the rule set aggregations are executed in this study following secure rule set transfers between intra and inter-region leaders. The vulnerability of beamforming data transmission to jamming attacks is considered analytically and via simulation, and contrasted with multichip routing. A cross-layer approach (physical reputation-based routing) which feeds physical-layer information into the reputation-based routing algorithm is presented, permitting candidate routes that make use of the best beamforming relays to be discovered. Outlier detection based on region is a very useful safety strategy for wireless sensor networks with a high number of scattered nodes. Developing a more effective outlier detection system in Wireless sensor networks (WSNs) can ensure that data packets are successfully transmitted without loss or corruption.

KEYWORDS: rule-sharing sessions, Enhanced Adaptive Acknowledgment, Wireless sensor networks (WSNs), network-layer, data packets, bandwidths/memory.

I. INTRODUCTION

Wireless sensor networks (WSNs) can achieve transmission when the network senses data between a node and another set of sensor nodes (SNs). During data transmission in WSNs, sensed data may require significant amounts of energy in terms of power consumption, energy dissipation, etc. The sensor nodes (SNs) gather the information through event monitoring from their environments and transfer it to the next SN or the base station (BS). However, WSNs obtain data from vulnerable deployment environments through the Internet or sensor actuators. WSNs are usually deployed in several applications such as battlefield surveillance, disaster recovery, healthcare applications, homeland security, agricultural monitoring, environmental monitoring, home automation, oil-refinery monitoring process, industry applications, etc. These WSN applications usually occur in vulnerable conditions. Each SN in a WSN is associated with resource constraints such as restricted battery power and limited resources. Securely aggregating sensed data via aggregator nodes plays a vital role in conserving energy efficiency in the network. In aggregating the sensed data, BS utilizes a security control mechanism. Secure data aggregation (SDA) uses security control mechanisms like authentication and authorization methods in WSNs. Thus, secure data aggregation ensures confidentiality, integrity, and availability for privacy preservation in a WSN while avoiding communication overhead (CO). Thus, secure data aggregation uses sensed data and avoids communication overhead. Consequently, SDA enhances the energy utilization of the SN during sensed data collection. In addition, SDA protocols play a vital role. They act as a firewall that should authenticate and authorize legitimate SN data for privacy preservation against any vulnerabilities or cyberattacks in the network. Due to this limitation of security control mechanisms such as secure node authorization, the lifetime of the WSN becomes a significant challenge. This challenge is due to the need to approve authenticated and authorized legitimate sensor nodes (SN) for secure data transmission in the network, which would subsequently lead to privacy concerns.

II. LITERATURE REVIEW

Uras Panahi (2023) The high volume of sensed and transferred data among nodes on wireless sensor networks makes it necessary to keep the data safe. This study offers an improved security mechanism, taking the application, security level, and bit error rate into account for wireless sensor networks. We used reserved bits of frame control field in the Zigbee MAC header to give the user the ability to choose between insecure or secure modes. Also, under particular circumstances (BER) using the cross-layered interaction mechanism, the network can switch to the other available

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205508 |

algorithms due to special criteria. We selected RECTANGLE, Fantomas, and Camellia algorithms and compared their performance against AES to provide an alternative security solution for different scenarios according to various security demands. The performance evaluations were measured and compared for the memory usage, throughput, battery consumption, and end-to-end delay metrics. Our results suggest using SPN-based block ciphers than the Feistel-based structure.

Nadeem Javaid (2022) In this study, an encryption and trust evaluation model is proposed on the basis of a blockchain in which the identities of the Aggregator Nodes (ANs) and Sensor Nodes (SNs) are stored. The authentication of ANs and SNs is performed in public and private blockchains, respectively. However, inauthentic nodes utilize the network's resources and perform malicious activities. Moreover, the SNs have limited energy, transmission range and computational capabilities, and are attacked by malicious nodes. Afterwards, the malicious nodes transmit wrong information of the route and increase the number of retransmissions due to which the SNs' energy is rapidly consumed. The lifespan of the wireless sensor network is reduced due to the rapid energy dissipation of the SNs. Furthermore, the throughput increases and packet loss increase with the presence of malicious nodes in the network. The trust values of SNs are computed to eradicate the malicious nodes from the network. Secure routing in the network is performed considering residual energy and trust values of the SNs.

Nadeem Javaid (2021) Wireless Sensor Internet of Things (WSIoTs) face various challenges such as unreliable data communication, less cost efficiency, security issues and high energy consumption due to their deployment in hostile and unattended environments. Moreover, the node's rapid energy dissipation due to the void holes and imbalanced network deployment has a bad impact on the network performance. To overcome the aforementioned issues, a blockchain based trust model for WSIoTs is proposed in this study. Moreover, the Dijkstra algorithm is used to propose a routing protocol for performing efficient communication between network nodes while simultaneously avoiding void holes between ordinary sensor nodes and a sink node. Furthermore, to provide transparency in the network, all the transactions performed by the nodes are recorded in the blockchain in an immutable manner.

Dionisis Kandris (2020) Wireless Sensor Networks are considered to be among the most rapidly evolving technological domains thanks to the numerous benefits that their usage provides. As a result, from their first appearance until the present day, Wireless Sensor Networks have had a continuously growing range of applications. The purpose of this article is to provide an up-to-date presentation of both traditional and most recent applications of Wireless Sensor Networks and hopefully not only enable the comprehension of this scientific area but also facilitate the perception of novel applications. In order to achieve this goal, the main categories of applications of Wireless Sensor Networks are identified, and characteristic examples of them are studied. Their particular characteristics are explained, while their pros and cons are denoted. Next, a discussion on certain considerations that are related with each one of these specific categories takes place. Finally, concluding remarks are drawn.

Mobile Sink Wireless Sensor Networks

In Mobile Sink Wireless Sensor Networks all the sensors are statically deployed to sense the environment and mobile sink traverse the networks. It overcomes the problem of the sink neighborhood problem as defined in previous section. In the sink neighborhood problem is neighbor nodes of sink participate more in the data transmission. The result is the faster energy deplete compared to other nodes in the network. If we look over the energy conservation model sensor deplete some amount of energy during the data receiving and the data transmission. As the sensor those are close to the sink, participate more data transmission i.e. for them and for those sensors away from the sink in the same direction. In MSWSN all nodes are static other than the sink in the network. Mobile sink traverse randomly to collect the sensor data. It may be collected with one hop or multi hop communication and our proposed model is the one hop data collection. As sink traversing throughout the network for data collection so the neighbor of the sink is not fix, so neighborhood problem will not arises.

Cluster based WSN architecture

In the cluster based WSN system, the target field is divided into a several groups, and each group is termed a cluster. Each of these clusters works as a flat based WSN system and select CH from among the sensor nodes, instead of BS. Sensor nodes send their sensed data to CH. CH collects the data and aggregates it and transfers it to the BS through other CH if it is not in the communication range of BS. For transmission static or dynamic route is selected. All sensor nodes should be in the communication range of BS is not a must.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205508 |

ID address Spoofing Attack

This type of attack comes under the Denial of Service (DoS) attack. Generally, in the message, the senders and the receiver's addresses are is written. The malicious node sends the packet to the receiver with another node's address as a sender. It hides its identity to misbehave in the network. Even though at the receiver side, it identifies that it is a false packet that is received, the remedial action, will be taken on the node whose address is stored in the packet, and its legal incoming packets may get rejected. The malicious node sends the random address of the legal nodes which are available in the network. Sometimes, the malicious node sends a request to send me huge data. So, according to the request the receiver sends data to the node whose spoofed address is written in the packet.

Replayed routing information Attack

The intruder steals the data from an authentic node and forwards the same message or a modified message after some duration to the destination. If it is not the current data then it is not useful for processing. This is called the replay attack. Objective of replay attack is to drain the energy of other nodes and disturb the processing at the receiver end. Replay attack can be avoided by using strong digital signatures.

Security Vulnerabilities and Protocol Goals

The cluster-based protocol (like LEACH) which are data transmission protocol for WSNs, are vulnerable to a many securities attack. In general, the attacks to CHs in CWSNs could produce a serious damage to the network, since data aggregation and data transmission rely on the CHs fundamentally. If an attacker manages to act as if it's a CH or negotiate the CH, it can provoke attacks such as sinkhole and selective forwarding attacks, thus upsetting the network. Alternatively, an attacker may intend to inject false sensing data into the WSN like pretending as a leaf node to transform the bogus information to the CHs. Since CHs are rotating from nodes to nodes in the network by rounds making it harder for external attackers to recognize the routing fundamentals as the intermediary nodes and attacks them. The properties in LEACH like decrease the risk of being attacked on intermediary nodes, and make it difficult for an external attacker to recognize and compromise important nodes.

III. RESEARCH METHODOLOGY

This methodology is used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and movement. Homomorphic encryption performs computations on ciphertext, thus generating an encrypted result which when decrypted matches sensor results of operations performed on plaintext. Each node in a sensor network encrypts the raw data and sends it to the next higher-level node or BS. The higher-level node performs computation on the received ciphertext and forwards to the next higher-level node. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The multiplicative property refers to the multiplication of two ciphertexts on decryption that yields the product of their plaintexts. The data integrity is also satisfactory because if any of the ciphertext is altered, it would not match the signature at the BS in the verification step. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN. In this, Efficient and Trustworthy data transmission is thus especially necessary and is demanded in many such practical wireless sensor networks. Aggregate signature method is a digital signature that is utilized to verify the signature of multiple users simultaneously in a single short signature, which reduces energy consumption. Protocols are proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

IV. RESULTS AND DISCUSSIONS

The stream ciphers usually encrypt bit by bit and for each bit encryption, they use different keys. The block ciphers are utilized to encrypt the block of data or files (64 to 128 bits in size) and the same key is used for encrypting each of the blocks. The patient is monitored for a period of time and his or her health data are transmitted as a block or file to the hospital. In SHS, the medical data are encrypted using symmetric block cipher. The most common symmetric algorithms, namely AES, Data Encryption Standard (DES), Rivest‟s Cipher 6 (RC6), Blowfish and International Data Encryption Algorithm (IDEA) are compared of their performance. Java is used for implementing the algorithms over the dataset given. The dataset have 130 observations and 3 variables which contain normal body temperature, gender and heartbeat rate.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

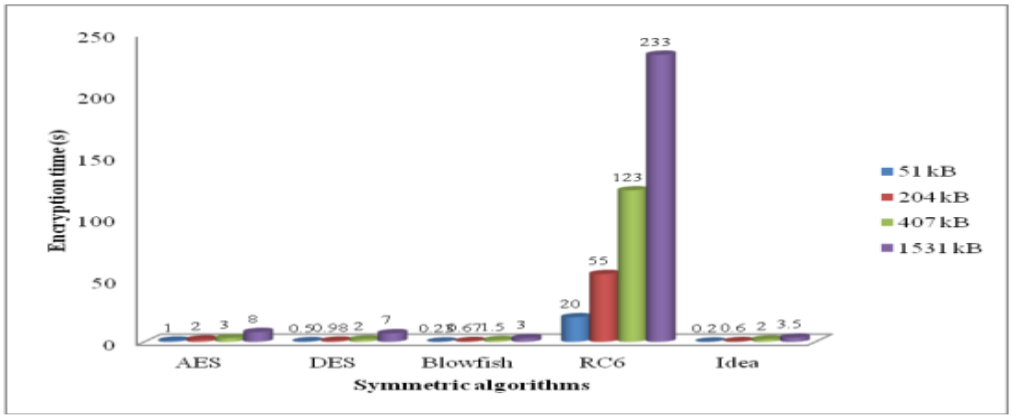
|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205508 |

Table 1 and graph 1 represents the encryption time, Table 2 and graph 2 shows the decryption time while Table 3 and graph 3 show the total computation time of the algorithms which include key generation, encryption and decryption time. From the performance analysis, the Blowfish has been found to have very less encryption and decryption time compared to the other algorithms. Since the medical data need to be transmitted within a short-span of time, the blowfish algorithm is used in SHS.

Table 1: Encryption time of symmetric algorithms

Symmetric algorithms	File size			
	51 kB	204 kB	407 kB	1531 kB
AES (s)	1	2	3	8
DES (s)	0.5	0.98	2	7
Blowfish (s)	0.23	0.67	1.5	3
RC6 (s)	20	55	123	233
Idea (s)	0.2	0.6	2	3.5



Graph 1: Encryption time of symmetric algorithms

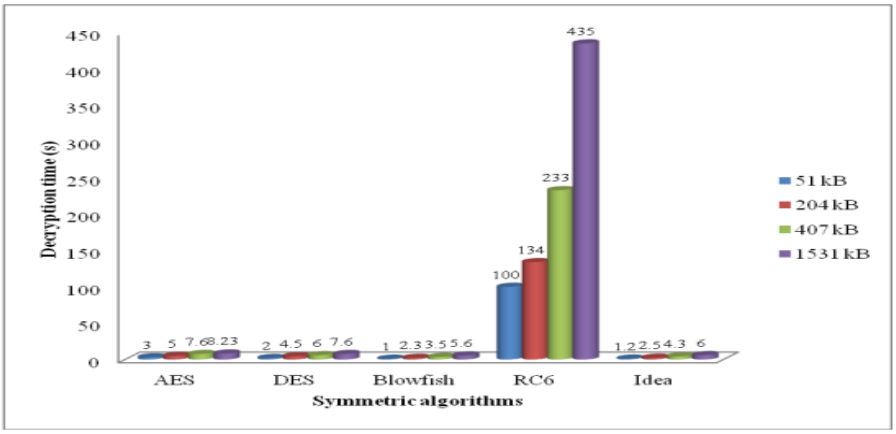
Table 2: Decryption time of symmetric algorithms

Symmetric algorithms	File size			
	51 kB	204 kB	407 kB	1531 kB
AES (s)	3	5	7.6	8.23
DES (s)	2	4.5	6	7.6
Blowfish (s)	1	2.3	3.5	5.6
RC6 (s)	100	134	233	435
Idea (s)	1.2	2.5	4.3	6

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

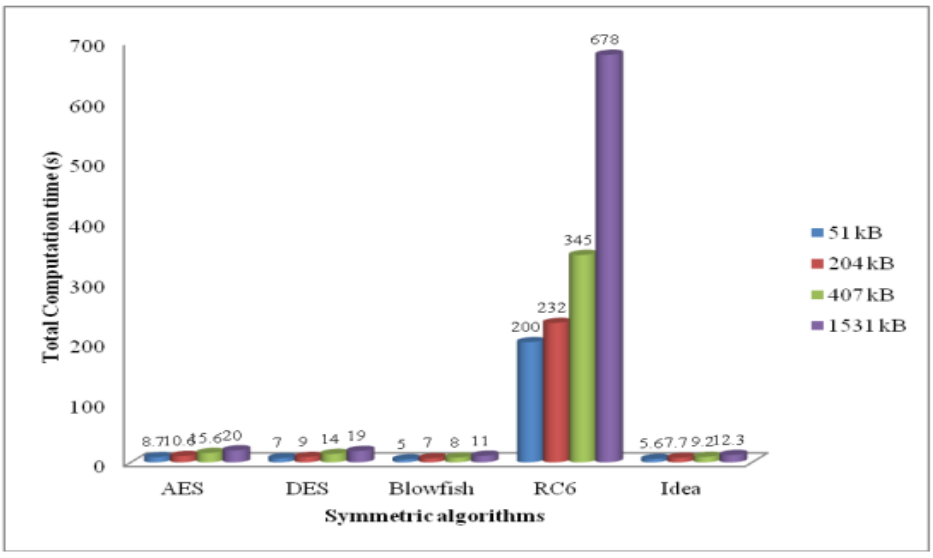
| DOI:10.15680/IJIRSET.2023.1205508 |



Graph 2: Decryption time of symmetric algorithms

Table 3: Total computation time of symmetric algorithms

Symmetric algorithms	File size			
	51 kB	204 kB	407 kB	1531 kB
AES (s)	8.7	10.6	15.6	20
DES (s)	7	9	14	19
Blowfish (s)	5	7	8	11
RC6 (s)	200	232	345	678
Idea (s)	5.6	7.7	9.2	12.3



Graph 3: Total computation time of symmetric algorithms

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205508 |

V. CONCLUSIONS

The computation time of security algorithms is directly involved in energy consumption of the network. So, the proposed security methods concentrate on providing security properties like data integrity, confidentiality and authenticity with less computation time. Extensive study is made to find out the suitable end-to-end encryption algorithm and aggregate signature techniques for securing sensor data. The combination of algorithms is implemented for temperature readings using the Intel lab dataset. The limitation of homomorphic cryptosystem is not recoverable and not suitable for block of different data types. The decryption time of homomorphic cryptosystems is also high. The homomorphic cryptosystems take a long time for decrypting medical data of different data types. So, a study is made on finding the suitable symmetric algorithm and access control techniques. Blowfish and CP-ABE are identified as the best and executed on the gender, body temperature and heart beat rate values. To extensively reduce the computation time for low powered devices, a study is made on the lightweight symmetric algorithms. To implement this task, a study is done on the layer of attacks, impact of attacks and rules to detect the attacks. The classification algorithms such as SVM, BPN and ELM are compared using NSL-KDD dataset. ELM is found to have high accuracy than SVM and BPN.

REFERENCES

1. Dionisis Kandris (2020), "Applications Of Wireless Sensor Networks: An Up-To-Date Survey", Appl. Syst. Innov., Issn:2571-5577, Vol.3(1), Pages.14. Https://Doi.Org/10.33 90/Asi3010014
2. George Xydis (2015), "Review Of Real-Time Electricity Markets For Integrating Distributed Energy Resources And Demand Response", Applied Energy, Issn:1872-9118, Vol.138, Pages.695-706.Https://Doi.Org/10.1016/J.Apenergy.2014.10.048
3. Joy Haughton (2017), "Blockchain Technology In The Chemical Industry: Machine-To-Machine Electricity Market", Applied Energy, Issn:1872-9118, Vol.195, Pages.234-246.Https://Doi.Org/10.1016/J.Apenergy.2017.03.039
4. Nadeem Javaid (2021), "A Secure And Efficient Trust Model For Wireless Sensor Iots Using Blockchain", Digital Object Identifier, Issn:0275-9527, Vol.10, Doi:10.1109/AC CESS.2022.3140401
5. Nadeem Javaid (2022), "Blockchain Based Secure Routing And Trust Management In Wireless Sensor Networks", Sensors, Issn:1424-8220, Vol.22(2), Pages.411. Https://Doi. Org/10.3390/S22020411
6. Uras Panahi (2023), "Enabling Secure Data Transmission For Wireless Sensor Networks Based Iot Applications", Ain Shams Engineering Journal, Issn:2090-4495, Vol.14, Issue.2, Https://Doi.Org/10.1016/J.Asej.2022.101866
7. Wattana Viriyasitavat (2019), "When Blockchain Meets Internet Of Things: Characteristics, Challenges, And Business Opportunities", Journal Of Industrial Information Integration, Issn:2452-414X, Vol.15, Pages.21-28. Https://Doi.Org/10. 1016/J.Jii.2019.05.002
8. Xu Wu (2021), "A Blockchain-Based Trust Management Method For Internet Of Things", Pervasive And Mobile Computing, Issn:1574-1192, Vol.72, Https://Doi.Org/10.101 6/J.Pmcj.2021.101330
9. Zhenghui Li (2017), "Facile Synthesis Of Ultrasmall Si Particles Embedded In Carbon Framework Using Si-Carbon Integration Strategy With Superior Lithium Ion Storage Performance", Chemical Engineering Journal, Issn:1873-3212, Vol.319, Pages.1-8. Https://Doi.Org/10.1016/J.Cej.2017.02.141

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details