International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1912-1917 www.ijaem.net ISSN: 2395-5252

Secure Patient Data Transmission Using Wireless Sensor Network

[1]Vetrimanikumar.J, [2]Sabitha.D, [2]Sharmila.S, [2]Sowmiya.K, [2]Thenpandi.B

[1]*Assistant Professor,Department of Electronics and Communication Engineering,SSM Institute of Engineering and Technology*

[2]*UG Scholar,Department of Electronics and Communication Engineering,SSM Institute of Engineering and Technology*

Submitted: 15-06-2022 Revised: 20-06-2022 Accepted: 25-06-2022

ABSTRACT
Wireless Sensor Networks (WSN) based healthcare systems are increasing day by day to advise the health status and living environment habitat of peoples. However, WSN based healthcare application suffers from the issues related to privacy and security. Susceptible attacks and security consideration comes into WSN based healthcare applications as an interesting and challenging problem. One of the challenges in WSNs is to provide high-security requirements with constrained resources. The security requirements in WSNs are comprised of node authentication, data confidentiality, anti-compromise and resilience against traffic analysis.In this paper, wehave proposed a privacy preservation scheme for WSN based healthcare application utilizing the principles of multipath routing, secret sharing and hashing. The healthcare data collected from the wireless sensor network is splits into n components. Further, the hash value is computed for each component with the help of well-known hashing technique. The change in hash value is used to detect changes in the message. These n components are then transferred to n servers, with the help of multipath routing. This article provides extensive simulations to validate new approach. Results show that secret splitting along with multipath routing helps to attain privacy preservation in WSN based healthcare system."

KEYWORDS: Elliptic curve cryptography, User Authentication, Access control, Wireless Sensor Networks

I. INTRODUCTION

The security of wireless sensor networks is becoming increasingly important as they grow more ubiquitous. This is especially true for products like medical sensors, where confidentiality is critical.The WSNs sensors are used to measure, monitor and record the patient's data such as blood pressure, heart rate, temperature and other vital data. These devices frequently communicate sensitive data, necessitating the use of a cryptographic technique that ensures data confidentiality and integrity, as well as the legitimacy of people using the sensor network's devices. All of these are provided by public-key cryptography; but, owing of computational and battery power limits, the most prevalent public-key algorithm (RSA) cannot be used because it is too computationally expensive. Because it requires substantially smaller key sizes, Elliptic Curve Cryptography (ECC) presents an option that provides comparable security strength withsignificantly less computation. Data encryption, digital signatures, user authentication, and other applications have all made substantial use of public-key cryptography. In comparison to the widely used symmetric key cryptography in sensor networks, public-key cryptography offers a more flexible and straightforward interface that requires no key predistribution, pairwise key sharing, or a sophisticated one-way key chain mechanism. However, there is a widespread perception in the sensor network research community that public-key cryptography is not feasible since the required computational intensity is incompatible with sensors with limited processing power and energy budget. The preliminary investigation appears to debunk this myth. The Wireless Sensor Network (WSN) is a self-organizing network that consists of a collection of sensor nodes that collect environmental data and communicate it to a sink or base station. The information can be gathered from the base station for further assessment. Sinks in

WSNs can be either static or dynamic. For some applications, a static sink is utilised as a battlefield environment, whereas a dynamic sink is used as a disaster management system.

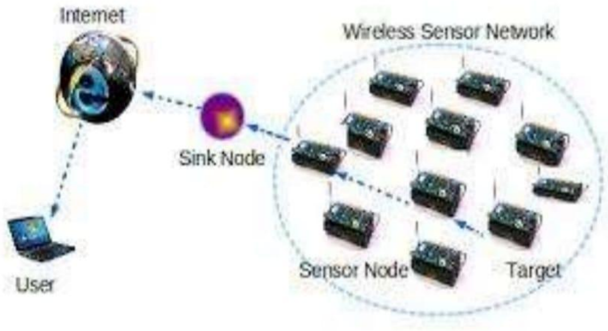


Fig. 1: WSN Architecture

II. RELATED WORK

1. F. McSherry and K. Talwar, "Mechanism design via differential privacy," in Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on, pp. 94–103, IEEE, 2007.
2. F. Eigner and M. Maffei, "Differential privacy by typing in security protocols," in Computer Security Foundations Symposium (CSF), 2013.

M. T. Hale and M. Egerstedty, "Differentially private cloud-based multiagent optimization with constraints," in American Control Conference, pp.1235–1240, 2015.

W. Zhang, R. Rao, G. Cao, and G. Kesidis, "Secure routing in adhoc networks and a related intrusion detection problem," in MilitaryCommunications Conference, 2003. MILCOM'03. 2003 IEEE, vol. 2,pp. 735–740, IEEE, 2016

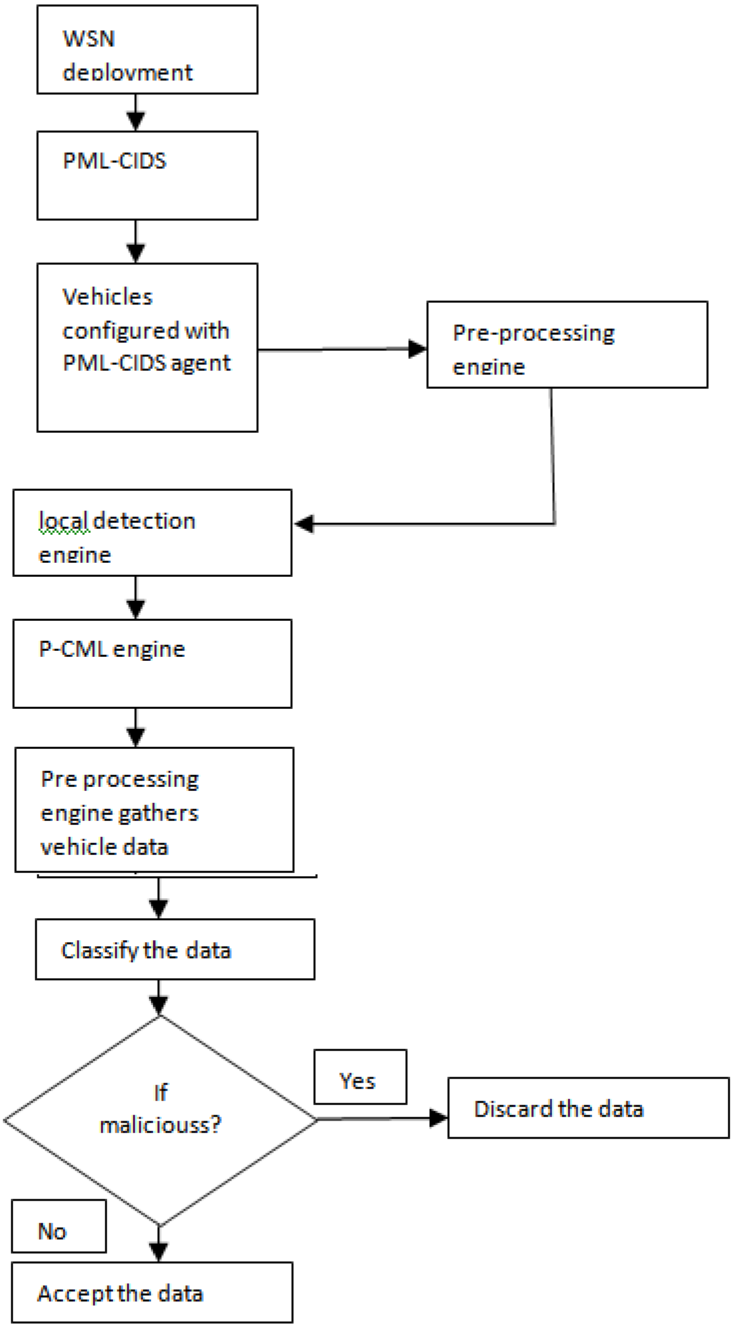
Z. Muda, W. Yassin, M. Sulaiman, and N. Udzir, "Intrusion detection based on k-means clustering and na¨ ıvebayes classification," in Information Technology in Asia (CITA 11), 2011 7th International Conference on, pp. 1–6, IEEE, 2016

S.-J. Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L. Lai,and C. D. Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," Expert systems with Applications, vol. 38, no. 1, pp. 306–313, 2017.

III. PROPOSED APPROACH

Proposed scheme implements Elliptic Curve Cryptography (ECC) for secure medical data transmission and key distribution.Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data.ECC focuses on pairs of public and private keys for decryption and encryption of web traffic. ECC is frequently discussed in the context of the Rivest–Shamir–Adleman (RSA) cryptographic algorithm.It has been proved that ECC is a better asymmetric algorithm than RSA due to level of security achieved by using small key size. Previously, proposed approach has used ECC, but replay attack and mutual authentication was major concern in that approach. Our proposed technique use ECC approach for secure data transmission and resolve these issues. Replay attack issue can be resolved using time stamp value. This value would enable receiver to identify the status of message. Real message would contain current time whereas replay attack message would contain old time. Apart from replay attack issue, mutual authentication is one of the most important requirements in WSNs due to the privacy and security concern of data. Proposed technique describes that Sink node would authenticate the base station serverbefore actual transmission of medical data and base station server would also authenticate the sink node before any actual reply. However, devices are having resource constraints, so large computations cannotbe performed because they may slowdown the overall performance.

IV. BLOCK DIAGRAM

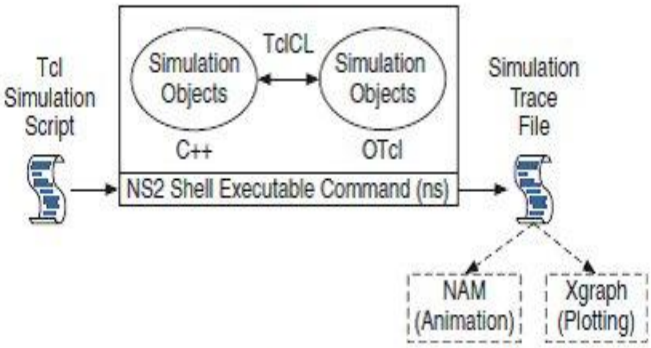


VI. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic algorithm. It is one of the most secure algorithms which includes very few computations and a very small key size, but achieves better security than other algorithms which include heavy computations and large key size. ECC provides same level of security with 112-bit key size in contrast to RSA with 512-bit key size. ECC encodes any message in form of co-ordinates on any plane curve. That plane curve is based on any cubic curve equation. ECC was proposed by Neil Koblitz and Victor Miller in 1985. Common equation of ECC is $y^2=x^3+ax+b$.Computations (which are involved in ECC) follow different steps for compute the results. Addition of two points on the curve is the reflection of intersecting point generated by the straight line passing through those two points.Multiplication is the repeated addition of points.Encoding of message in form of points on curve has powerful security because of computations.

V. SYSTEM ARCHITECTURE

NS2 provides users with an executable command "ns" which takes one input argument, the name of a Tcl simulation scripting file. In most cases, a simulation trace file is created and is used to plot graph and/or to create animation. NS2 consists of two key languages: CCC and Object-oriented Tool Command Language (OTcl). While the CCC defines the internal mechanism (i.e., a backend) of the simulation, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The CCC and the OTcl are linked together using TclCL. Mapped to a CCC object, variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle is just a string (e.g., "_o10") in the OTcl domain and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped CCC object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts with users and other OTcl objects. It may define its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures (instprocs) and instance variables (instvars),respectively. Before proceeding further.



Basic architecture of NS.

VII.MODULES

1. Implementation of WSN and Qos Analysis

In this module, a WSN is implemented. Nodes are randomly deployed in the network area. Nodes are moving in inconsistent speed in different direction. Data communication is enabling and data packets are transmitted between the vehicular nodes. The malicious node is randomly selected and configured. The malicious nodes are configured to attract and disturb the data

2. Implementation of PML-CIDS scheme

The pre-processing engine gathers and pre-processes the real-time WSN system data that describe the system activities in a vehicle. If the user of the vehicle requires the current classifier to be updated, then the P-CML engine is initiated. The local detection engine uses the newly retained classifier to analyze the system data. Otherwise, the current classifier is used in the classification of intrusions. If any intrusion is classified, the alarm is triggered.

3. Performance analysis

In this module, the performance is analyzed on both the implementations. The results are logged in a separate trace file. The values for the parameters like delay, throughput, energy and overhead are analyzed. The results are plotted into xgraphs and analyzed.

4. Intrusion detection systems (IDSs):

Intrusion Detection System is important devices that can mitigate the threats by detecting malicious behaviors. Furthermore, the collaborations among vehicles in WSNs can improve the detection accuracy by communicating their experiences between nodes.

VIII. FUTURE WORK

Developing, An Intrusion detection tool (Software) , using method proposed through this research. • Investigating, applicability of unsupervised data mining techniques for intrusion detection. • Developing, a system that operates with a more global scope may be capable of detecting distributed attacks or those that affect an entire enclave. Development of such a system would be a valuable contribution to the study of intrusion detection. +This study was carried out using supervised data mining techniques. Supervised Classification algorithms such as J48 decision tree, rule based One R and bayes net algorithms. So further investigation needs to be done using other classification algorithms such as Neural Networks and Support Vector Machine plus using association rule discovery.

IX. RESULT

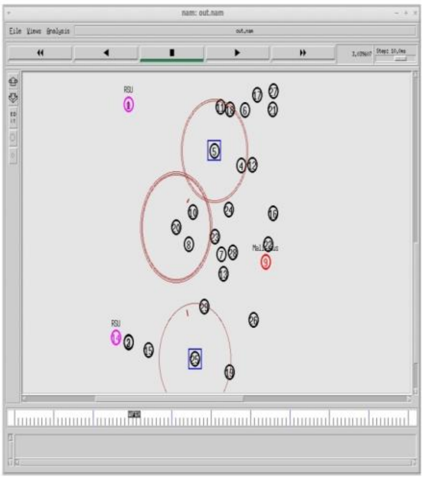


Fig 1.Detecting malicious node using elliptic curve Cryptography in Wireless Sensor Network

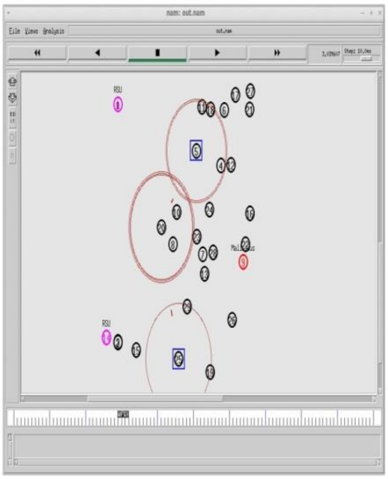


Fig 2.Setting safer path to send the data in Wireless Sensor Network

X.GRAPH

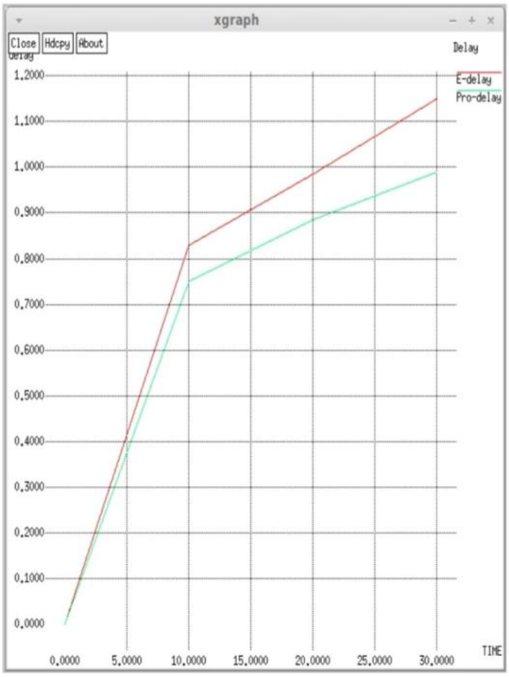


Fig 3.Delay graph of output

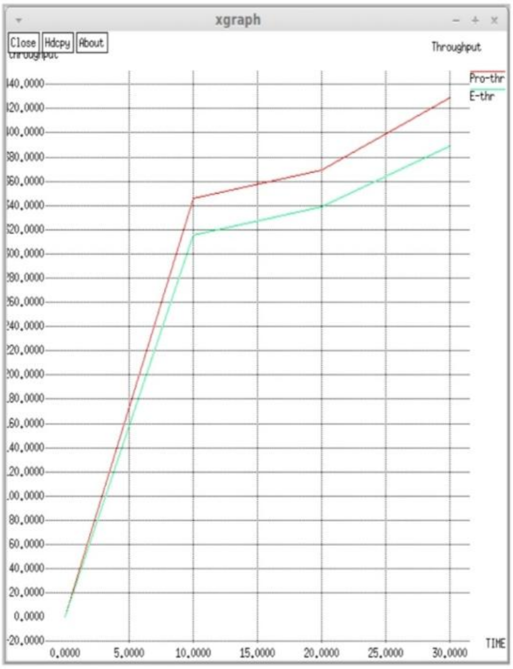


Fig 4.Throughput graph of output

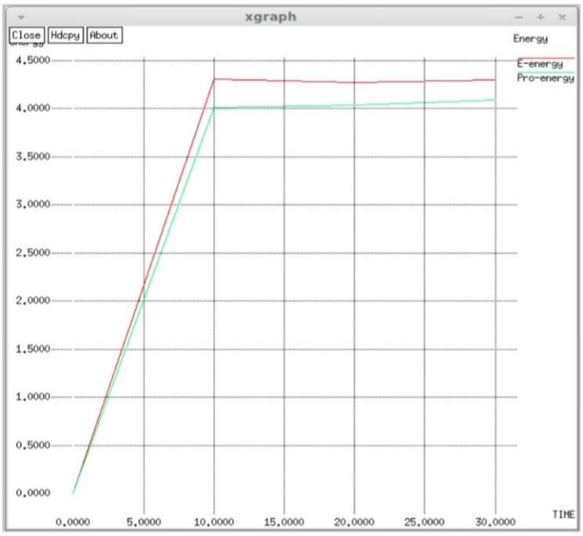


Fig 5.Energy graph of output

IX. CONCLUSION

WSNs are widely utilised in a variety of vital applications, so securing them has been a top focus for the research community. An elliptic curve-based security Our signcryption-based protocol uses the least computing time for the gateway in contrast to existing protocols while delivering the same or higher security level, making it appropriate for security and privacycritical WSN applications.protocol for WSNs is provided in this work, which successfully provides user anonymity, secrecy, mutual authentication, and safe key formation while consuming less computational time than existing related systems. The proposed protocol also protects against offline dictionary attacks, insider attacks, impersonation attacks, replay attacks, and stolen verifier attacks, according to the researchers.

REFERENCE

[1]. W. Zhang, R. Rao, G. Cao, and G. Kesidis, “Secure routing in adhoc networks and a related intrusion detection problem,” in Military Communications Conference, 2003. MILCOM’03.2003 IEEE, vol. 2, pp. 735–740, IEEE, 2003.

[2]. T. Anantvalee and J. Wu, “A survey on intrusion detection in mobile ad hoc networks,” in Wireless Network Security, pp. 159–180, Springer, 2007.

[3]. C. J. Fung, Q. Zhu, R. Boutaba, and T. Bas¸ar, “Bayesian decision aggregation in collaborative intrusion detection networks,” in Network Operations and Management Symposium (NOMS), 2010 IEEE, pp. 349–356, IEEE, 2010.

[4]. Q. Zhu, C. Fung, R. Boutaba, and T. Basar, “Guidex: A game-theoretic incentive-based mechanism for intrusion detection networks,” IEEE Journal on Selected Areas in Communications, vol. 30, no. 11, pp. 2220– 2230, 2012.

[5]. A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN,WMN, WSN. CRC press, 2016.

[6]. Alshamsi AZ, Barka E (2017) Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks. In: International Conference on Informatics, Health & Technology (ICIHT).

[7]. Malik MS, Ahmed M, Abdullah T, Kousar N, Shumaila MN (2018a) Wireless body area network security and privacy issue in e-healthcare. Int J AdvComputSciAppl 9(4):209–215.

[8]. [8]Hathaliya J, Sharma P, Tanwar S, Gupta R (2019) Blockchain-based remote patient monitoring in healthcare 4.0. In: 2019 IEEE 9th International Conference on Advanced Computing (IACC). Tiruchirappalli, India, 13–14 Dec, 2019.

[9]. Sandhu A, Malik A (2020) PAP: priority aware protocol for healthcare application in wireless body area network. Int J Recent TechnolEng (IJRTE) .