Investigation on Cryptosystem and Hash Based Multifactor Authentication Techniques in Wireless Sensor Network

C.VENKATACHALAM[1], DR. A. SURESH[2]
[1] *Ph.D (Part time) Research Scholar, Dept. of Computer Science, Periyar University, Salem*
[2] *Head, Dept. of Computer Science, Sona College of Arts and Science, Junction Main Road, Salem*

Abstract- ***Transmission of information between the clients in the network is a significant part of today, client of the network needs to share their data between different clients of verified information transmission. They were numerous method of exchange o information were done, however verified degree of information exchange is a significant angle what everybody needs. Mystery information transmission is as yet serious issue in network. Implanting the mystery data is an overhauling innovation for sharing mystery information, inserting process cryptography technique assumes a key job. Successful inserting of mystery information by utilizing visual cryptography helps a ton for mystery information transmission. This paper gives the review of different cryptographic techniques and its viability for secure transmission over network.***

Indexed Terms- ***Cryptography, Protocol, Accuracy, Traffic, Intensity.***

I. INTRODUCTION

A wireless sensor network (WSN) is a network of spatially scattered little or small devices, called sensor nodes or bits, which are equipped for detecting physical and ecological conditions, for example, sound, weight, temperature, light and moistness. The sensor nodes are self-governing in working, resource-compelled in nature with less processing capacities and live on batteries. WSNs additionally comprise of uncommon nodes called as gateway nodes (GWN) or base stations which are wealthy in registering abilities and capacity resources. The sensor nodes move the detected data to the gateway nodes, through various nodes, utilizing radio transmission, for further handling. To set up mystery pair wise keys between two neighbor sensor nodes in WSNs, the key pre-distribution method is utilized. It is accomplished by the mainstream protocol, called the bootstrapping protocol. The bootstrapping protocol must not just empower a recently conveyed sensor hub to start a protected correspondence with the current sensor nodes, yet it should likewise permit sensor nodes sent sometime in the not-too-distant future to join the network. As of late, there are new advancements in the region of open key cryptography for resource obliged situations that actualize elliptic bend cryptography with less control utilization and computational prerequisites. Thus, ECC is doable for structuring security protocols in resource-compelled sensor nodes. In any case, most scientists in this network still acknowledge that a symmetric figure is the best decision for encryption/unscrambling of the information in WSNs. The issue of key appropriation turns into a difficult undertaking because of resource restrictions of sensor nodes just as their helplessness to physical catch by a foe in an objective field.

Figure 1: Wireless Sensor Network Security Protocols

The gateway nodes or the cluster heads, present in the WSN, gather the ongoing information from sensor

nodes and stores it in their memory which the genuine clients can inquiry. Be that as it may, since the GWNs gather the information from sensor nodes in normal interims, the information present at the GWNs may not be the ongoing information and such information can significantly be valuable for measurable purposes or for examination as it were. Henceforth, it is likewise required for the clients to speak with the sensor nodes straightforwardly to gather the ongoing data. To speak with the sensor nodes straightforwardly, the client needs to verify against the gateway nodes just as the sensor nodes to guarantee the safe correspondence. Given the resource-crunchy nature of sensor nodes, it is basic to structure proficient confirmation plans with no trade off in security.

II. LITERATURE SURVEY

[1] Sreevidya R C, Nagaraja G S [2018]: Proposed to Secure Multicast Routing for Wireless Sensor Networks using ACO-AODV with DHKE Cryptosystem. The ACO-AODV-DHKE algorithm accurately transmit data from Source to Destination (S-D) by evaluating better throughput, Packet Delivery Ratio (PDR), Packet Loss (PL), End-to-End Delay (E-ED) and Energy Consumption (EC) in secured environment. ACO is utilized for dynamic clustering in heterogeneous environment versatile SNs to transmit data using multicast routing among CH and sink node. Route establishment using AODVRP and Diffie–Hellman Key Exchange Algorithm (DHKE) is utilized for secured data transmission in versatile sensor networks. Also, the need of each node storing all Public keys is diminished in this manner minimizing the overhead on each node. The performance of the ACO-AODV-DHKEWSNs procedure will be evaluated as far as End to End delay, through-put, Packet Delivery Ratio, and Packet Loss, and Energy Consumption. ACO-AODV-DHKE strategy is executed in NS2 to achieve better enhanced clustering for data transmission using ACO-AODV algorithm. The potentials of multicast routing protocol in routing the data from source to various destinations. Also, the clustering mechanism using ACO demonstrated as one of the promising clustering approach. The security essentials using DHKE demonstrated that the key management system gave a secure and safe environment for the data packets. In considering all these strategies the routing protocol develops to be an efficient protocol when compared to against various parameters, for example, throughput, packet delivery ratio, packet loss, start to finish delay and energy consumption. [2] Yong Xu, Fen Liu [2018]: Proposed a Hybrid Key Management Scheme for Preventing Man-in-Middle Attack in Heterogeneous Sensor Networks. A hybrid key management scheme (NHKM) based on ECC and symmetric cryptosystem, achieving authentication of the node's public key by using certificates and nonce signature, can well avoid man-in-middle (MIM) attack. proposes a hybrid key management scheme (NHKM), where BS and the SINK utilize public key encryption based on ECC. Authentication of the node's public key is achieved by using certificates and nonce signature. And ordinary nodes and the cluster head, the cluster head and SINK utilize symmetric key encryption. This plan avoids MIM attacks and performs well in asset cost, arrange connectivity, scalability and versatility. The NHKM scheme achieves the authentication of the public key between the SINK node and BS by using the certificate and the nonce signature. On the basis of, the SINK node is added between the cluster head and the base station, which avoids the large amount of asymmetric encryption between the cluster head and the base station, which guarantees the security as well as increases the system scalability. [3] Wanda Zhang, Tuanfa Qin, MessaykabewMekonen, Weichao Wang [2018]: Proposed a Wireless Body Area Network Identity Authentication Protocol Based on Physical Unclonable Function. The physical unclonable function module is added to the sensor of the remote body territory systems, and a vitality sparing, realtime sensor authentication protocol is proposed. an authentication system of remote body territory systems based on physical channel qualities is proposed, this instrument can exploit physical channel attributes, effectively oppose malignant assaults that carted out by the impersonation assailant away body without expanding communication overhead and additional equipment. Going for antagonistic assault that sensors on the body counterfeit different sensors to send false information in remote body zone systems, proposed a lightweight detection conspire, this plan can enormously improve systems security execution and adequately identify the on-body sensor impersonation assault by physical channel attributes and question response instrument. Base on physical

channel attributes. To make internet-of-things hardware and controllers increasingly viable an identity authentication substantially more secure, applies physical non cloning functions to Internet-of - things gadgets and proposes an authentication protocol based on physical unclonable function (PUF). [4] Leelavathi G1 , Shaila K, Venugopal K R [2018]: Proposed an Implementation of Public Key Crypto Processor with Probabilistic Encryption on FPGA for Nodes in Wireless Sensor Networks. To structure Public Key Crypto Processor with modification of Public Key Algorithms, RSA and ECC for Wireless Sensor Node engineering considering velocity, time and region as the plan parameters. The proposed Public key Crypto algorithm is modeled utilizing Verilog and blended on Spartan 3 and 6, Virtex 7, Kintex 7 and Artix7. proposed framework, algorithm is created to actualize Public Key Crypto Processor (PKCP) on FPGA to conquer the territory utilization issue and increment the speed. Here, the region and throughput are trade off that makes it appropriate for Wireless Sensor Node communication.The proposed and built up a Public Key Crypto Accelerator for WSNs bits in which complete encryption of 164 piece data operations are accomplished in one single clock cycle with exceptionally low region and computational time. Combinational way postponement isn't found in any module implementation. In the proposed methodology, the computation time is diminished in this way diminishing the vitality consumption and zone utilization thusly expanding the system lifetime. The implementation model of the PKCP framework includes the plaintext to ASCII conversion, Elliptic Curve parameter Generator, Mapping and Probabilistic Encryption to deliver figure content. The figure content is transmitted over the unsecured channel. To acquire the first plaintext Probabilistic Decryption is performed first pursued by demapping and conversion of ASCII esteems to starting content. The relative investigation of territory and speed is done regarding the gadget utilization and computational time. The exhibition is assessed regarding throughput rate. Crypto processor is given probabilistic highlights that make the algorithm safe against animal power and picked figure content assaults, along these lines giving adequate quality against crypto investigation. [5] Jian Li, Yun Liu, Zhenjiang Zhang, Bin Li, Hui Liu, Junjun Cheng [2018]: Proposed an Efficient ID-based Message Authentication with Enhanced Privacy in Wireless Ad-hoc Networks. propose an efficient message authentication with enhanced privacy (IMAEP) plot based on ring mark and identity based signature. To demonstrate that other than unconditional privacy, the proposed plan can accomplish enhanced privacy which can guard against full key introduction assault. propose an efficient message authentication with enhanced privacy (IMAEP) plot based on the identity based ring mark scheme. This plan can accomplish enhanced privacy, which can guard against full key introduction assault, while keeping unconditional privacy. Contrasted with the plan proposed in with a similar degree of enhanced privacy, the plan can hold unconditional privacy with much lower computational overhead. The security definition of the IMAEP plan incorporates two folds: anonymity which is identified with the privacy of the plan, and unforgeability which is identified with the credibility of the mark. The proposed IMAEP plan can give unconditional source anonymity, anonymity against full key introduction assault, and existential unforgeability against the adaptive picked message-and-identity attack. To assess the presentation of the proposed IMAEP conspire. Since the plan proposed accomplishes the equivalent enhanced privacy which is the anonymity against full key introduction assault, we will look at the presentation between these two plans. The comparison for the quantities of major numerical operations during marking and confirming. proposed an efficient message authentication with enhanced privacy (IMAEP) plot based on the identity based ring mark scheme. [6] Norah AlMansour, Dr.Saad Alahmadi [2018]: Proposed a Secure Ad Hoc On-Demand Distance Vector Routing Protocol in WSN. The intend to improve the security of WSN steering protocol. Ad Hoc On Demand Distance Vector (AODV) directing protocol by structure a security layer that uses Paillier homomorphic cryptographic component; to ensure sending bundle data and steering during the communication and convey data respectability and confidentiality. The responsive protocol is on-demand steering protocols that find the route once required, AODV is a case of the receptive protocol. It is a generally utilized which based on a distance vector steering protocol. Conventional AODV does not consider security objectives, for example, uprightness to guarantee that directing

bundle isn't changed during travel. To give confidentiality and Integrity of directing parcel by presenting SL-AODV which altered AODV by structure a security layer in AODV utilizing Paillier homomorphy encryption. After to executed the proposed protocol, multiple simulation tests to look at the exhibition of SLAODV by doling out various estimation parameters. The pace of the effectively sent message through a communication channel after some time, which called throughput. A line chart that watches the node numbers over throughput for SL-AODV. Throughput brings about SL-AODV uncover that system utilization increment as node numbers increment. Another way, that expands security in WSN directing by utilizing cryptography. proposed protocol SL-AODV, adjusting AODV by structure a security layer utilizing cryptosystem Currently, security in the WSN is a functioning territory of research that has pulled in a lot of attention because of quickly developing of WSN applications. [7] E.H. Teguig, Y. Touati and A. Ali-Cherif [2017]: Proposed an ECC based-Approach for Keys Authentication and Security in WSN. Propose another component for public keys management utilizing an elliptic curves cryptosystem where the goal is to enhance medicines by decreasing essentially the calculation of scalar multiplications. In this manner, public keys trade component permits a partial communication by transmitting just the abscise and the LSB of the ordinate of the elliptic curve point totaling 161 bits instead of 320 bits. To building up a powerful approach for key authentication and management utilizing the concept of elliptic curves cryptosystem. Setting up a mystery key between two sensor nodes as per Diffie-Hellman trade on ECC requires two scalar multiplications. Other than of noteworthy essential time required for scalar multiplication calculation, Diffie-Hellman trade experiences man-in-the-center assault cause public keys can't be verified directly. A vigorous cryptosystem improvement permitting a key authentication by executing a concept of elliptic curves. The system requires two stages for its implementation: pre-arrangement stage and post organization or recognition stage. So as to demonstrate the adequacy of the proposed instrument for key authentication utilizing the concept of ECC, performed exploratory tests on a TMote Sky sensor with a similar report to three different components: An Elliptic Curve Digital Signature Algorithm, which is a digital mark algorithm used to verify a digital content, An Integrated Encryption Scheme Elliptic Curve to give semantic protection from picked plain content and picked figure content assaults, and Elliptic curve Diffie–Hellman that uses a secure key trade algorithm by means of a non secure channel. proposed a strong methodology, which is based on elliptic curves cryptosystem where the goal is to improve arrange power against assaults. [8] S.Subha, UGowri Sankar [2015]: Proposed a Message Authentication And Wormhole Detection Mechanism In Wireless Sensor Network. proposed a novel and effective worm opening detection based on RTT. While guaranteeing message sender privacy. RTT can be connected to any message to give message content legitimacy and then node traded off assault. To give jump by bounce message authentication without the shortcoming of the work in square gap assault. proposed jump by bounce message authentication plan based on RTT. At the point when connected to the remote sensor coordinate with fixed number of sink nodes, in potential methods for traded off node identification. To contrast the proposed plan and MES plot through simulation utilizing NS-2 simulator. The simulation results demonstrate that the framework has satisfactory scope of execution and pertinence. Both hypothetical and simulation result demonstrates that, in similar situation, the proposed plan is increasingly effective then the MES plot as far as computational overhead, vitality consumption, message postponement and memory consumption. To recognize the wormhole assault which is based on the RTT of the message between progressive nodes and their neighbor numbers.

III. EXPERIMENTAL RESULTS

- Accuracy Ratio

LEACH	Hybrid Key Management Scheme	Homomorphic Encryption Alg	AODV
11	7	33	20
25	15	47	33
39	23	56	43
46	36	61	5

50	42	70	64

Table 1: Comparison table of Accuracy Ratio

The Comparison table of Accuracy Ratio of LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV shows the different values. While comparing the LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV, the AODV algorithm is better than the other three algorithms. The LEACH algorithm value starts from 11 to 50, Hybrid Key Management Scheme values starts from 7 to 42, Homomorphic Encryption Alg values starts from 33 to 70 and the AODV algorithm values starts from 20 to 64. Every time the AODV value gives the great results.

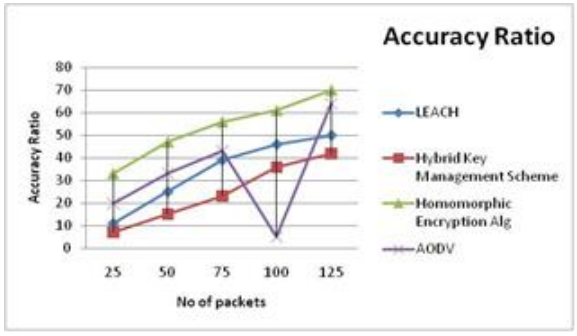

Figure 2: Comparison chart of Accuracy Ratio

The Comparison chart of Accuracy Ratio of LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV demonstrates the different values. No of packets in x axis and Accuracy Ratio in y axis.The AODV algorithm is better than the other three algorithms. The LEACH algorithm value starts from 11 to 50, Hybrid Key Management Scheme values starts from 7 to 42, Homomorphic Encryption Alg values starts from 33 to 70 and the AODV algorithm values starts from 20 to 64. Every time the AODV value gives the great results

- Intensity Ratio

LEACH	Hybrid Key Management Scheme	Homomorphic Encryption Alg	AODV
4	15	19	7
8	21	27	13
12	29	35	19
16	38	44	25
20	46	50	31

Table 2: Comparison table of Intensity Ratio

The Comparison table of Intensity Ratio of LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV shows the different values. While comparing the LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV, the AODV algorithm is better than the other three algorithms. The LEACH algorithm value starts from 4 to 20, Hybrid Key Management Scheme values starts from 15 to 46, Homomorphic Encryption Alg values starts from 19 to 50 and the AODV algorithm values starts from 7 to 31. Every time the AODV value gives the better results.

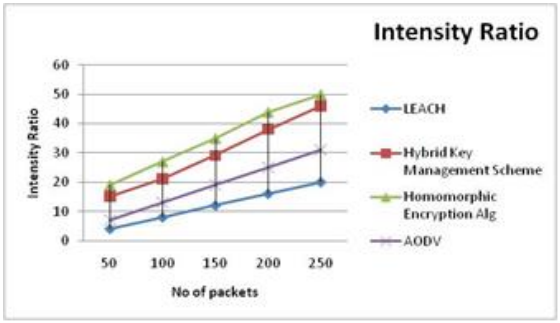

Figure 3: Comparison chart of Intensity Ratio

The Comparison chart of Intensity Ratio of LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV demonstrates the different values. No of packets in x axis and Intensity Ratio in y axis.The AODV algorithm is better than the other three algorithms. The LEACH algorithm value starts from 4 to 20, Hybrid Key Management Scheme values starts from 15 to 46, Homomorphic Encryption Alg values starts from 19 to 50 and the AODV algorithm values starts from 7 to 31. Every time the AODV value gives the better results.

- Traffic Ratio

LEACH	Hybrid Key Management Scheme	Homomorphic Encryption Alg	AODV
0.21	0.15	0.34	0.78
0.28	0.22	0.43	0.97
0.32	0.28	0.49	1.02

0.38	0.35	0.55	1.11
0.44	0.41	0.62	1.28

Table 3: Comparison table of Traffic Ratio

The Comparison table of Traffic Ratio of LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV shows the different values. While comparing the LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV, the AODV algorithm is better than the other three algorithms. The LEACH algorithm value starts from 0.21 to 0.44, Hybrid Key Management Scheme values starts from 0.15 to 0.41, Homomorphic Encryption Alg values starts from 0.34 to 0.62 and the AODV algorithm values starts from 0.78 to 1.28. Every time the AODV value gives the great results.

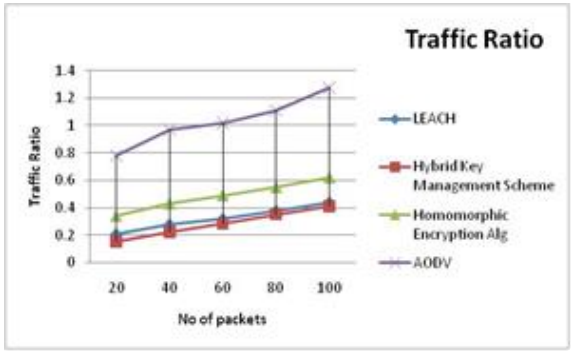

Figure 4: Comparison chart of Traffic Ratio

The Comparison chart of Traffic Ratio of LEACH, Hybrid Key Management Scheme, Homomorphic Encryption Alg and AODV demonstrates the different values. No of packets in x axis and Traffic Ratio in y axis.The AODV algorithm is better than the other three algorithms. The LEACH algorithm value starts from 0.21 to 0.44, Hybrid Key Management Scheme values starts from 0.15 to 0.41, Homomorphic Encryption Alg values starts from 0.34 to 0.62 and the AODV algorithm values starts from 0.78 to 1.28. Every time the AODV value gives the great results.

CONCLUSION

Network assumes a significant job for moving the information or data starting with one gathering then onto the next. Moving the information faces the security issue, while moving the information may release or misfortune because of the outsider of the interloper in the network. For mystery information transmission is as yet serious issue in network. Inserting the information for mystery data is a redesigning innovation for sharing mystery information, numerous systems were proposed by numerous creators utilizing cryptography, stegnography, and so on, which give a few disadvantages. From our investigations paper gives the review of different cryptographic strategies and its adequacy for secure transmission over network through visual cryptography technique which gives progressively secure of information transmission over the network.

REFERENCES

[1] Sreevidya R C, Nagaraja G S," Secure Multicast Routing for Wireless Sensor Networks using ACO-AODV with DHKE Cryptosystem", Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018) IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3.

[2] Yong Xu, Fen Liu," Hybrid Key Management Scheme for Preventing Man-in-Middle Attack in Heterogeneous Sensor Networks", 2017 3rd IEEE International Conference on Computer and Communications

[3] Wanda Zhang, Tuanfa Qin, MessaykabewMekonen, Weichao Wang," Wireless Body Area Network Identity Authentication Protocol Based on Physical Unclonable Function", 2018 International Conference on Sensor Networks and Signal Processing (SNSP) ieee.

[4] Leelavathi G , Shaila K, Venugopal K R," Implementation of Public Key Crypto Processor with Probabilistic Encryption on FPGA for Nodes in Wireless Sensor Networks",ieee 2018.

[5] Jian Li, Yun Liu, Zhenjiang Zhang, Bin Li, Hui Liu, Junjun Cheng," Efficient ID-based Message Authentication with Enhanced Privacy in Wireless Ad-hoc Networks", 2018 International Conference on Computing, Networking and Communications (ICNC): Communications and Information Security Symposium

[6] Norah AlMansour, Dr.Saad Alahmadi," Secure Ad Hoc On-Demand Distance Vector Routing Protocol in WSN", ©2018 IEEE

[7] E.H. Teguig, Y. Touati and A. Ali-Cherif," ECC based-Approach for Keys Authentication and Security in WSN", 2017 9th IEEE-GCC Conference and Exhibition (GCCCE)

[8] S.Subha, UGowri Sankar," Message Authentication And Wormhole Detection Mechanism In Wireless Sensor Network", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015

[9] Yassine Essadraoui, Mohamed Dafir Ech-cherif El Kettani," Wireless sensor node's authentication scheme based on Multivariate Quadratic Quasi-groups", ©2015 IEEE

[10] Leelavathi G , Shaila K, Venugopal K R," Elliptic Curve Crypto Processor on FPGA using Montgomery Multiplication with Vedic and Encoded Multiplier over GF(2m) for Nodes in Wireless Sensor Networks", 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS),

[11] Abiramy N V, Smilarubavathy G, Nidhya R, Dinesh Kumar A," A Secure and EnergyEfficient Resource Allocation Scheme for Wireless Body Area Network", ©2018 IEEE

[12] Leron Lightfoot, Jian Ren," R-STaR Destination-Location Privacy Schemes in Wireless Sensor Networks", IEEE ICC 2015 - Communication and Information Systems Security Symposium.

[13] Min Thant, Than Myo Zaw," Authentication Protocols and Authentication on the Base of PKI and ID-based", ©2018 IEEE

[14] Karlo Knezevi," Combinatorial Optimization in Cryptography", MIPRO 2017, May 22- 26, 2017, Opatija, Croatia IEEE 2017

[15] Renuka Suryawanshi," H-WSN with Maximized QoS using Secure Data Aggregation",IEEE 2016.