Mutual Authentication of Nodes in WSN using Migrated ECC of Asymmetric Key

[1]B. TAMILARASI, MCA, M.Phil., (Ph.D), [2]DR. R. UMARANI, MCA, M.Phil., Ph.D,
[1] Research Scholar(RM12CS44), SCSVMV University, Kanchipuram.
[2] Associate Professor of Computer Science, Sri Saradha College for Women, Salem -16.
[1]arasi21373@gmail.com,
[2]umainweb@gmail.com.

***Abstract*— Wireless Sensor Networks (WSNs) are a promising innovation for a few modern and everyday applications. The advancement of remote sensor systems was spurred for use in reconnaissance in a war zone by military applications. These days WSN systems are utilized as a part of modern industrial applications for monitor and control the process flow, to monitor machine health, in consumer applications and so on. A couple to a few a huge number of junctions are comprised in WSN, where every junction is associated with one or now and again more sensors. There is a need for an approach that prevents unauthorized nodes from using the network to communicate the legitimate nodes or Internet. This will probably reduce most of the security attacks that can be happened. Some systems use Elliptic Curve Cryptography(ECC) for authentication process, because small size of key used for encryption. However, ECC have some disadvantages. The primary problem in ECC is, it significantly makes encrypted message greater in size which makes this mechanism more complex. Furthermore, it is difficult to implement when compared to other public key encryption techniques and also it provides less security alone. To overcome difficulties in ECC, this system introduces Migrated ECC that uses asymmetric key. This system consist of node registration, distribution of authorized node list to all legitimate nodes, and mutual authentication of nodes in different networks, and handover of node from one network to other. From our assumption, it proves that Migrated ECC performs better than ECC in terms of security and efficiency.**

Keywords: Wireless Sensor Networks, Mutual Authentication, Security Attack, Migrated ECC.

I. INTRODUCTION

A WSN is an extraordinary sort of remote correspondence arranges comprising of various quantities of geologically appropriated self-ruling gadgets utilizing sensors to screen physical or natural conditions. This framework contains a passage junction which goes about as a halfway junction that gives remote network back to the wired world and circulated nodes for the purpose of sending WSN data to different types of networks.WSN is utilized as a part of Military and national security applications, Environment checking, and Medical applications. Wireless Sensor Networks used in many applications due to its low cost, tiny size and ease of deployment [1]. In any case, there are a few security difficulties to be overcome to completely understand the favorable circumstances because of ubiquitous nature of WSN. Correspondence being communicated in nature is more inclined to various sort of assaults like eves dropping, capture, infuse and change transmitted information [2]. WSN systems are described by little size, a substantial number, and minimal effort. It is obliged by vitality, computational power, and correspondence data transmission and capacity. Little size suggests little battery, ease and low power CPU, radio with least data transfer capacity and range [3].

Conventional cryptographic calculations utilizing open key are exceedingly asset concentrated to specifically fit into the WSN engineering [4][5]. Hence ECC has risen as a computationally effective plan for asset imperative sensor equipment stage particularly in IOT and Smart City applications [6][7][8]. Among all the security primitives, validation is an essential prerequisite, which may likewise cover information trustworthiness, information freshness, and sequencing. Excepting certain cases including military and observation, classification may not be the vital as the verification would be [9][10].

Elliptic Curve Cryptography is an optional way to deal with people in general key cryptography systems like RSA. Elliptic Curve Cryptography is based on elliptic curve theory using discrete logarithms and it creates smaller but faster cryptographic keys which can be shared among large numbers of users.ECC helps to establish security in lower computing power and battery resource usage; it is becoming widely used for mobile applications. ECC give proficient execution of remote security highlights, for example, secure mailing and web perusing, however, has a few burdens when contrasted and other cryptography procedures.ECC expands the extent of the scrambled message is substantial when contrasted and RSA encryption. Moreover, the ECC calculation is more intricate and hard to actualize than RSA. ECC is a type of open key cryptography, in which one encryption key, names as a private key, is kept the mystery, while another, named as an open key, is uninhibitedly appropriated. Open key cryptography requires more calculation than private key encryption, it

utilizes just a single, shared encryption key. In remote gadgets, open key cryptography may abbreviate the lifetime of batteries or of the gadgets themselves. Be that as it may, open key cryptography is more secure than private key cryptography. So we propose migrated ECC to overcome burden when using public key in WSN for authentication purpose.

II. SYSTEM BACKGROUND

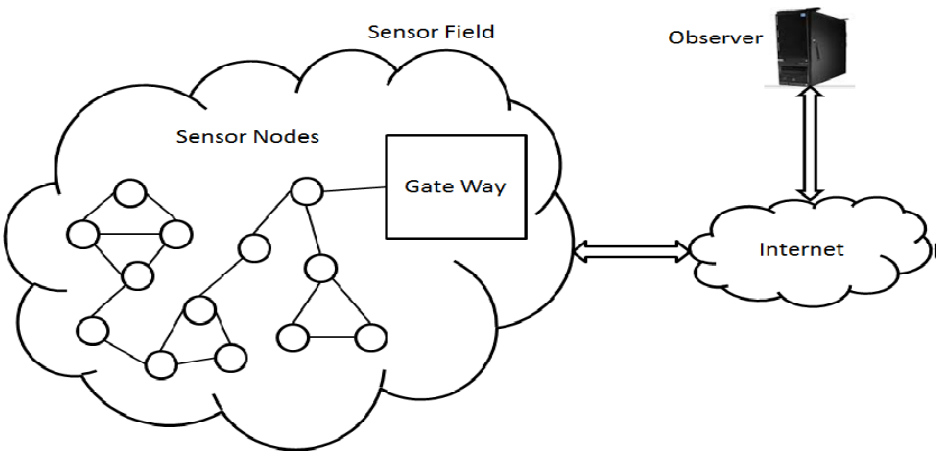
A. WSN System Architecture

A WSN is a system of numerous sensor junctions where every junction coordinated with a sensor to identify physical wonders, for example, light, warm, weight, and so on. WSNs are viewed as an uprising data gathering strategy to assemble the data and correspondence framework which will extraordinarily enhance the dependability and proficiency of foundation frameworks. Compared to the wired solution, WSNs provide easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

A WSN is depicted as a system of junctions that helpfully sense and may control the earth, empowering collaboration between people or PCs and the encompassing condition [11]. WSN incorporates sensor junctions, actuator hubs, passages, and customers. A substantial number of sensor hubs sent arbitrarily within or close to the checking territory (sensor field), shape arranges without anyone else association. Sensor junctions screen the gathered information and transmit to other sensor junctions by jumping. Amid the procedure of transmission, checked information might be taken care of by numerous hubs to get to passage hub after multi hop steering, lastly achieve the administration hub through the web or satellite. The client arranges and deals with the WSN with the assistance of administration hub; distribute checking procedure and accumulation of the observed information. As related technologies mature, the cost of WSN equipment has dropped dramatically, and their applications are expanded from the military areas to industrial and commercial fields.

Traditionally security is built to protect the confidentiality, integrity and availability of network data in TCP/IP networks. It protects the system from malicious attacks which can lead to malfunctioning systems and information disclosure and makes the system reliable. As the normal for junction and application condition, WSN security needs customary security insurance, as well as the uncommon prerequisites of put stock in, security and protection.

WSNs require security protection of integrity, availability, confidentiality, non-repudiation, and user privacy. It supports system integrity, reliability by protecting the system from malicious attacks. WSNs may need to protect the nodes against tampering, protect the communication channel, and routing in the network layer [12]. TSP logging/ audit functions may be required to detect attacks. Security aspects in WSNs consist of message authentication, encryption, access control, identity authentication, etc. Security of WSNs may be categorized as follows: junction security, crypto calculations, key administration, secure steering, and information conglomeration [13] [14].



These days, WSNs interface the foundation of physical elements firmly with the data arranged harm to the framework, (for example, control, transportation, concoction plant and national security) by infection dangers will bring about unfathomable outcomes.WSN is usually more exposed to various security threats because unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. TSP issues must be considered appropriate from the earliest starting point. The dangers to which a WSN is uncovered must be somewhat tended to by organizing security advancements. The safeguard against complex assault shapes, for example, Sybil, Dos, and irregular junctions is not agreeable [15].

B. Migrated ECC

Circular bend cryptography is a technique for scrambling information records with the goal that exclusive particular people can unscramble them. ECC depends on the science of elliptic bends and uses the area of focuses on an elliptic bend to encode and decode data. ECC gives productive execution of remote security highlights, for example, secure email administrations and Web perusing yet has a few inconveniences when contrasted and other cryptography methods.ECC decreases the size of encryption key but increases the size of encrypted message. And ECC mostly used with private key cryptography, because it takes less cost, computation but open key cryptography is more secure and more mind boggling than private key cryptography framework. So we move to Migrated ECC to overcome difficulties in public key ECC and provide better security.

III. AUTHENTICATION FRAMEWORK DESIGN

The proposed confirmation system has been intended to allow only registered nodes in communication and perform mutual authentication before communication.

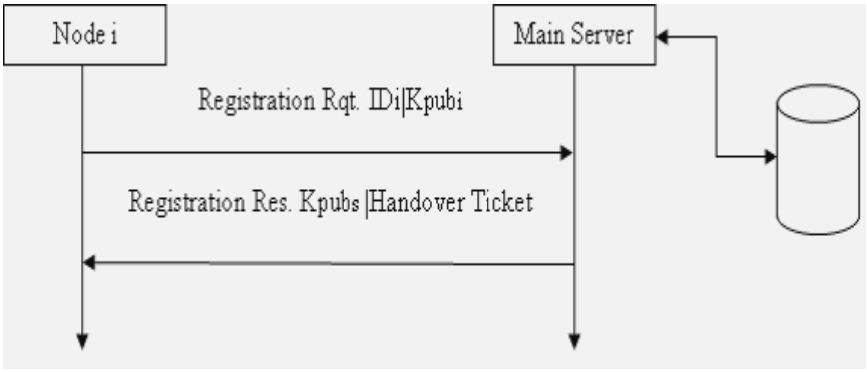
- Network Admission Control Solution scheme [16] performs registration and authentication of new nodes entered in wireless network. But it does not provide mutual authentication before node to node communication. Asymmetric key cryptography is more secure than symmetric key cryptography because to key are involved, but this system uses symmetric key to encrypt/decrypt the exchanged messages.
- Yue ui and Maode Ma˝s scheme [17] perform mutual authentication and keyestablishment using elliptic curve diffie-hellman cryptography. But it involves more message exchanges between nodes in network with server for mutual authentication. It perform mutual authentication between nodes only, no authentication to server in networks.

The proposed framework tends to the above issues and traverses the structure over the accompanying 4 stages: Registration phase, Distribution of Authorized Node List phase, Mutual Authentication phase, and Handover phase.

A. Registration Phase

In this phase node that want to communicate with nodes in sensor network first register itself with server for further communication. New node registers its id and public key to server. Now server stores id and corresponding public key in authorized node list table and returns acknowledgement to new node that is registered.

Server generates handover ticket it is used when one node moved from one sensor network to another sensor network. This handover ticket is used for fast authentication ofnode when handover is performed. Server sends handover ticket and its public key along with acknowledgement of registration. This ticket can be used for only one handover after that it will be expired. Server generates handover ticket again for same node when it is moved successfully to another network

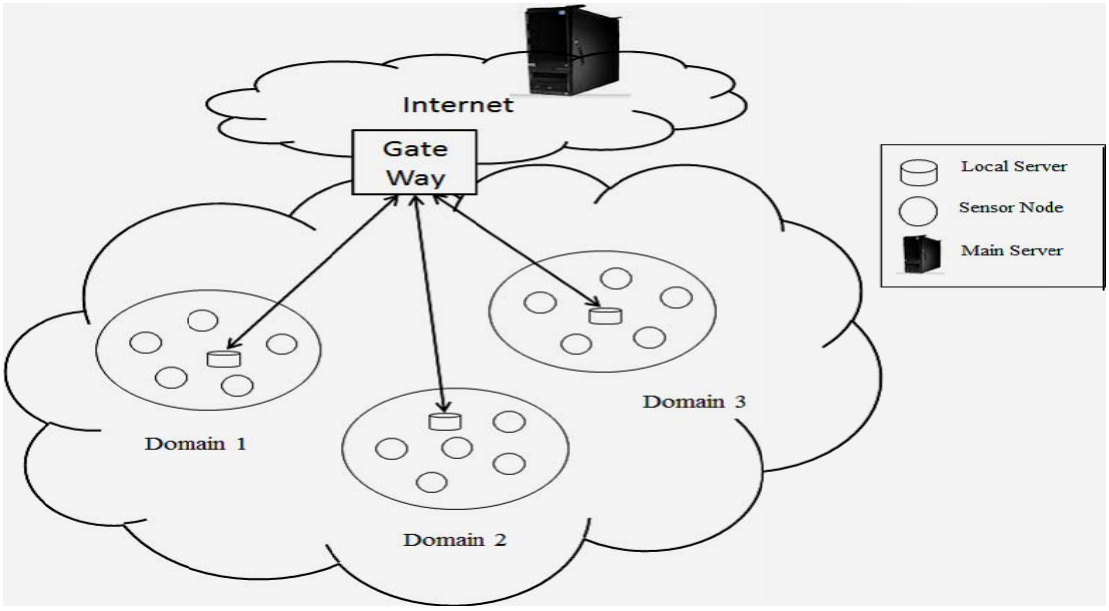


B. Distribution of Authorized Node List Phase

Whenever the authorized node list in main server changes, it is distributed to all currently active legitimate nodes in that network. Message with authorized node list is sent both periodically and when authorized node list is changes. Upon reception of this message, each node replies with acknowledgement message. Server local to a network sent error message to Main Server if it does not receive acknowledgement message after three retries. These messages are encrypted by corresponding node's public own private key.

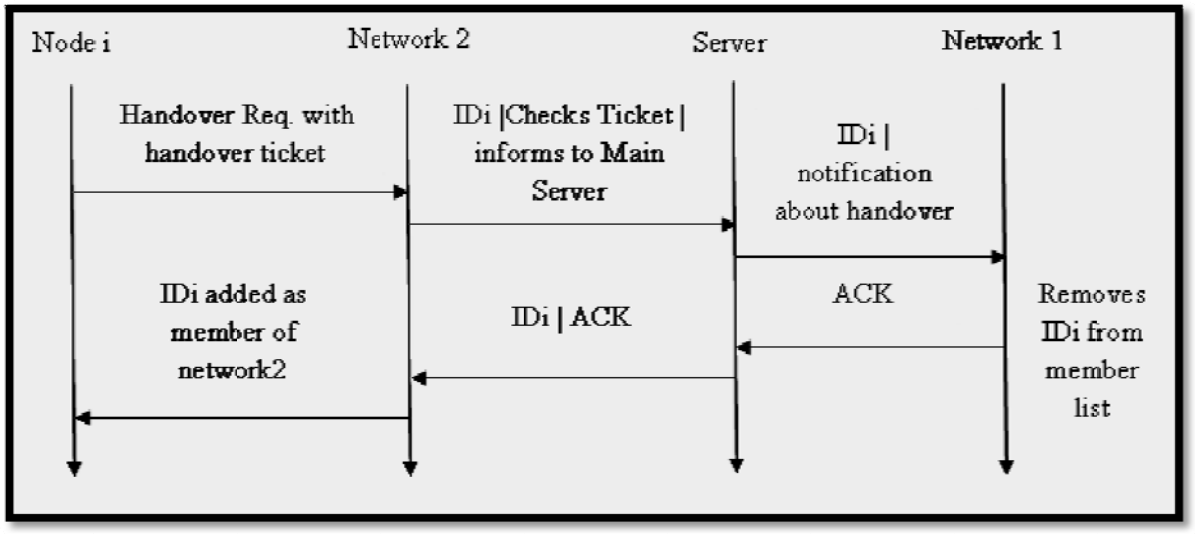
C. Mutual Authentication Phase

When a node called N1 in one network wants to communicate with node called N2 in another network, then both network's local servers are authenticated via gateway that connect these networks. Gateway performs mutual authentication of two parties involved in communication. First sender verifies existence of receiver and use receiver's public key retrieved from the main server to encrypt the message. On receiving message, receiver checks that message is from legitimate one by using authorized node list, if not the message is discarded. Otherwise it receives the message and decrypts it using its own private key.



D. Handover Phase

When one node moved from one sensor network to another network, that node uses its handover ticket for fast authentication. When mobile sensor node called N1 moves from area of network1 to network2, it will send a handover request to network2 through gateway. Upon receiving handover request network2 first make sure whether the ticket is expired. If so, the request is discarded. Otherwise, the network2 communicates with main server to verifies nodes id and inform about handover request. Server then sent notification to network1 to inform that node N1 is no longer in its area. Then local server in network1 checks if node N1 is out of its range and deletes the device from its member list and sent acknowledgement to main server. After receiving acknowledgement from network1, handover request is accepted and node N1 is added to member list in network2



IV. CONCLUSION

Security is the key factor of success of WSN. The proposed scheme gives security by mutual authentication between nodes involved in communication using migrated ECC. Use of public key cryptography enhances the security of WSN. Registered nodes only considered as authorized nodes and communication is limited only to authorized nodes. The main server maintains list of registered nodes with their id and public key. Authentication process performed when nodes moved to another network, handover ticket is used for this purpose. When one node wants to communicate with another one, it gets public key of that node and encrypt the message using that key and send. Once the message is received, receiver uses its own private key and decrypts the message. It also permit communication of nodes in different networks with mutual authentication performed at gateway which connect theses networks.

REFERENCES

[1] Akyildiz IF, et al.”A survey on sensor networks,” IEEE Communications Magazine, 2002,40(8): PP. 102-114. 3104.
[2] Adrian Perrig, John Stankovic, David Wagner,” Security in wireless sensor networks” Communications of the ACM June 2004 vol 47, no. 6, pp 53-57.
[3] Memsic,CrossBow Xserve User Manual May 2007.
[4] J. Hill et al., ”System Architecture Directions for Networked Sensors, ”ASPLOSIX: Proc. 9th Int‟l. Conf. Architectural Support for ProgrammingLanguages and Operating Systems, New York: ACM Press, 2000, pp. 93-104.
[5] J. Hill et al., ”System Architecture Directions for Networked Sensors,”SIGOPS Oper. Syst. Rev., vol. 34, no. 5, 2000, pp. 93-104
[6] Andrea Zanella and Lorenzo Vangelista ,”Internet of Things for Smart Cities,“ IEEE INTERNET OF THINGS JOURNAL, Vol 1,No 1, February 2014.
[7] D. Cuff, M. Hansen, and J. Kang, “Urban sensing: Out of the woods,” Commun. ACM, vol. 51, no. 3, pp. 24–33, Mar. 2008.
[8] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz. “Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs,” CHES2004, volume 3156 of LNCS, 2004.
[9] Xu Huang, et al. “Fast Scalar multiplication for Elliptic curve cryptography in Sensor Networks with Hidden Generator point,” 2010 International conference on Cyber- enabled distributed Computed and knowledge Discovery.
[10] D. Hankerson et al,.” Guide to Elliptic Curve Cryptography” Springer 2004.
[11] BRORING, A. et al. New generation sensor web enablement. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652.
[12] BLILAT, A., BOUAYAD, A., CHAOUI, N. and EL GHAZI, M. Wireless sensor network: Security challenges. Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 6872. Available from: http://novintarjome.com/wp-content/uploads/2014/05/Wireless-Sensor- etwork.pdf.
[13] JAIN, A., KANT, K. and TRIPATHY, M. R. Security solutions for wireless sensor networks[C]. Proceedings of the 2012 Second International Conference on Advanced Computing and Communication Technologies (ACCT „12). IEEE Computer Society, 2012, pp. 430433.
[14] WANG, Y., ATTEBURY, G. and RAMAMURTHY, B. A survey of security issues in wireless sensor networks IEEE Communications Surveys and Tutorials 8, 2006, pp. 223.
[15] WOOD A. D. and J.A. Stankovic. 2002. “Denial of Service in Sensor Networks.” IEEE Computer, 35 (10), 54-62.
[16] Luis Miguel L. Oliveria, Joal J. P. C Rodrigues and Victor M. Denisov, Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms, VOL. 12, NO. 6, December 2016.
[17] Y ue iu and Madode Ma, Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks, VOL. 12, NO. 6, December 2016.