Secure User Authentication and Data Transfer in Wireless Sensor Network Using Elliptical Curve Algorithm and Data Session Using MD5

[1]Pooja Gupta, [2]Shashi Bhushan, [2]Sachin Majithia,
[1]Research Scholar, Department of Information Technology, Chandigarh Engineering College, Landran,India
[2]Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, India

***Abstract*- Wireless sensor networks (WSN) are self- governing sensors that are widely distributed in the respective environment. They are also referred as wireless sensor and actuator networks (WSAN). They are used to observe physical or environmental conditions, for example, temperature, sound, natural activities etc. They collect data from each active node and pass it to the network to the centralized location. There are many problems in wireless sensor network like user authentication as well as data travel in the network is not so much secure. We are developing a technique in which firstly we are allowing the user to pass the hard security authentication scheme and then the user can join the network. This technique allow user to authentically deploy node in the wireless sensor network and securely send data from source to destination. Further we are also providing a secure file transmission in network via public and private key concept. In this way the secure and authenticated transmission of data in prescribed environment is achieved.**

***Index Terms*- Data Transmission, Wireless Sensor Networks, Cryptography, Authentication, Encryption.**

I. Introduction

Wireless sensor Networks are specific type of ad-hoc network which contains various nodes having sensor unit, communication unit which is wireless, a power unit and embedded processor. These networks are probable to be composed of many and possibly thousands of small sensor nodes, running independently without access to renewable energy. The rise of sensor network as one of the leading technology development in the coming eras has modeled many exclusive challenges to researchers [6]. Wireless sensor network can be arranged in different topologies like star, cluster and mesh network. But this increases the complexity of network and also energy consumption is always the main concern for the wireless sensor network. This motivates the researchers to implement large scale wireless sensor network in extremely complex uses. As sensor nodes are deployed in unreceptive environments, the security of the data like authenticity, confidentiality and integrity should be secured [12]. Some challenges that can be faced in wireless sensor networks are the energy of the nodes working in the network can be limited and less hardware resources are available. Environment in which the network is configured also plays a vital role in efficiency of network, if the environment is unreliable, that type of arrangement can not be considered noble for transmission of data. Hence, due to some issues related to wireless sensor network structure, we need to work on the allied areas of concern. Energy maintainance is important parameter as it signifies the longevity of the network lifetime. We encrypt the data to maintain the data authenticity and security. We ensure the secure data transmission from source to destination using private and public key encryption. This decreases the chance of entering of any information loss or alteration when drifting from one node to another. Also, we work on node deployment that should be secure enough so that no black node can enter in the network. Therefore, work can be done to enhance the security of the network so that secure transmission of information can be achieved from source to destination in the network.

II. Related Work

Wireless sensor networks are implemented in hostile conditions so there is always a concern about its security and integrity. S. Gopikrishnan and P. Priakanth suggested hybrid secure data aggregation (HSDA) to deliver highly protected data collection in an energy efficient way [12]. They basically work on energy efficiency calculations for achieving the secure data aggregation. It also works on node validity, data secrecy and data reliability in wireless sensor network. Omar Cheikhrouhou classified the current wireless sensor network schemes in three sections- centralized, contributory and hybrid. Contributory arrangement had benefit of fault-tolerance but at the outflow of computational cost .Whereas hybrid arrangement had adequate efficiency and fault-tolerance capability [10]. The work proposed the strategies that assist user to select the most appropriate SCG scheme depending on the limitations of wireless sensor network and necessity of application. The confidentiality of the data is the main concern for better performance. In this work, the reliability is maintained by detecting the missing packets during the transmission of data from source to destination [11]. Matteo Gaeta ,Vincenzo Loiab and Stefania Tomasiello assured the reliability of integrated compression encryption scheme in the cubic B-spline F-transform, which is guaranteed work for wireless sensor network security [8].

Cryptography is the mechanism which is used for secure communication in the network from source to destination. It is useful for protecting information in the network when the information is passed through the active nodes in the established environment. It is basically the way to hide and validate the information which is transmitted in any respective environment. It sums up with protocols, algorithms and also prevents the unauthorised access of unwanted or suspicious intruders who can affect the delicate

information. It also allows the feature of authorising and verifying each component in the network. Kakali Chatterjee, Asok De and Daya Gupta anticipated a shared authentication protocol which is based on timestamp that creates a new session key for respective session. This authentication scheme is based on ECC which executes user authentication and also resolves the key management difficulties. This process needs low computational as well as communication load and consumes less energy. They preserve security by secret key generation and avoid susceptible attacks, which also recovers delay and traffic congestion issues in the wireless sensor network [7]. The overhead of generation of key for every session which can be challenged when heavy traffic is present on the network. Including this, session hijacking is also possible during data transmission. Encryption consists of the process in which the information is converted in indecipherable form for the one who doesnot have a decryption key to decrypt it. The one who doesnot have the key to decrypt, is unable to read and modify the information, which in return guarantees the security for the network. ECC is based on arithmetic structure of elliptical curves on the Galois field which contains the finite number of components. It is an implementation of public key cryptography and involves smaller keys compared to non- ECC cryptography which are grounded on plain finite fields, for offering comparable security. Elliptical arcs are valid for encryption, electronic signatures, pseudo-random generators etc. It is used in various cryptographic applications like Lenstra elliptic curve factorization, in which ECC is applied in integer factorization algorithms. This is also used with different encryption methods like RSA and Diffie –Hellman, to provide more security in the arrangement. It also uses low computing power and battery resource to provide satisfying security in the network. Hence, this can be effortlessly used in the wireless sensor network as it is favourable for the transmission of information which needs to be required less energy to be used. ECC is based on equations which is evaluated by applying operations on two members of the system to derive third member. S. Gopikrishnan and P. Priakanth implements end to end symmetric key cryptography for secure authentication using shared public key and uses hop by hop asymmetric key cryptography with private keys of respective node for data integrity and confidentiality. They put forward the private key generation and encryption at the leaf node that lessens the communication and computation overhead of nodes. The paper show work on energy efficiency calculations for achieving the secure data aggregation. It also works on node validity, data secrecy and data reliability in wireless sensor network [12]. This increases the overhead of encryption at each hop which on the other hand decreases the performance level. Achieving encryption at each hop can lead to overhead of calculating hash values again and again. This increases the problems in transferring the data as it increases the cipher text size of the data. On the other hand, it also rises the extra effort for decrypting the encrypted data at each node. Simultaneously, it also decreases the overall energy efficiency of the arranged network. But the work done shows a great potential to improve the security in the network.

Albert Levi and AbdülhakimÜnlü proposed the two tier key redistribution approach, in which the keys are distributed to every sensor node in the particular environment for secure communication [1]. In this, node deployment is done on the basis of zones comprises Agent (higher capacity node) and Regular nodes. It shows work on communication cost and minimum memory consumption using the minimum flooding mechanism during key distribution. The nodes that belongs to different zones have non-overlapping key information and can communicate via Agent nodes. It also show work on balancing overhead when the number of nodes and sensor field size is increased. They implement Blom's scheme for key distribution among nodes. Node deployment can be done with the most secured way as the data is transferred from these nodes in the network. One entry of any black node can affects the reliability of the framework by varying the information that is transmitted over the network. Ashok Kumar Das proposed that multi-phase deployment key establishment (MPDKE) for multi- phase deployment in large scale distributed sensor network. The paper demonstrates work on refreshing of deployed node's key rings before another deployment phase arises. It also provides high flexibility against node capture and better network performance. In this multi-phase deployment, the node will never retain static during their lifetime. The calculations provide improved trade-off between the connectivity of network, overheads and network flexibility in contradiction of node capture attacks [2].

Authentication plays a vital role in evaluation of reliability and security of the wireless sensor network. It is the way to provide secure session to the user,so that no black node can access the important and secret information of any other user. It doesn't allot any task for any user or what the user can see, it is simply the identification process and verification of the user who wants to access the information. Bakkiam David Deebak proposed secure-cum-efficient mutual adaptive user authentication (S-Cum-EMAUA) for hybrid wireless sensor network. It is robust for possible attacks and provides shared authentication, user privacy and session key establishment. It implements hash function and X-OR operations for evaluating real time client server system. The papers shows results on service response time, average end-to-end postponement, RTP and network consumption. They also works on the security of the network and computational proficiency of the authenticity of the network [4]. Matteo Gaeta, Vincenzo Loiab and Stefania Tomasiello proposed that a cubic B- spline F-transform to obtain higher accuracy, even when data are not associated and a lesser computational cost. In paper the work is compared with the lossless compression scheme for efficiency parameter. The arrangement explained in the paper is so secure that if an unauthorized user had an access to any specified parameter, then the security will not be affected. For recovery, they referred Keat, A. Samsudin and Z. Zainol research work in which wavelet based encoder is used with RC4 encryption algorithm [5]. Cubic B-Splines also improves the performance of F-transform based data compression. The results are concluded which gives high accuracy and low computational cost of final LS approach. It also assures reliability of the integrated compression encryption scheme [8].

As wireless sensor networks consists of nodes which are working in the network, therefore, the energy consumption parameter should be maintained. It should be as lower as it can be possible. Multiple paths can be used to avoid the load on one node of the network and to increase the network lifetime. To ensure energy efficiency, collisions can be avoided hence the work on collision of data packets in the network can also be considered. Any node can not be idle and over hearing in the network this affects the energy parameter of the network. Yang Yu and Viktor K. Prasanna works on diminishing the utmost energy dissipation over total nodes in the network while postulating a definite latency restraint [13]. On the other hand, this increases the transmission latency of the network which is again a major parameter. Min, Manish Bhardwaj, Seong-Hwan Cho, Eugene Shih, Amit Sinha, Alice

Wang and Anantha Chandrakasan works on the low energy signaling of the active network. They evaluate the tradeoffs between quality and energy dissipation among the nodes [9]. Ali Tufail projected that three tiered multi hop scheme has been introduced. First level of sensor nodes is for sensing, second level of relay nodes is for relaying and third level of gateway nodes is for managing the cluster and communicating to and from the cluster. With this node and network lifetime can be increased. Energy consumption reduction and less end to end hops are achieved in this research. In this a reliable and failure prone path is created from source to sink communication [3].

In above related work we encounter the discussions on various parameters and issues related to the wireless sensor networks. Security and authenticity are the major concern for any wireless sensor network, for this we use cryptographic algorithms as stated in above discussion [7] [12]. Energy efficiency is another area where we observed that by decreasing the energy consumption of the node in the wireless sensor network, we can enhance the overall performance of the network and also the lifetime of the node is improved. Lifetime enhancement also supports the reliability of the network and consistency of the network is also attained. Wireless sensor network performance can also be boosted by managing the appropriate topology of the network which should not be too much complex that affects the output of the arranged network.

III. Summary

Wireless sensor network is wide-ranging area where challenges and opportunities are present to work upon. When the data is passed from multiple hops then the encryption at each end can be modified and replaced by suitable algorithm which guarantees the secure transmission in the network [12]. We can explore the node deployment by working on more authenticated distribution of nodes in the network. If the extreme nodes are corrupted or attached maliciously then it can affect the whole network, hence, authentication and security is another challenging issue for wireless sensor network [1]. In related studies, very potential work is done on the parameters of wireless sensor network performance, for example, energy efficiency of the node in the network, security issues of data which is transmitted from one node to another in the wireless sensor network, bandwidth used while transferring the information in the network etc. Node authentication is the main concern for any wireless network because node is the only way to transfer information from source to destination as we can see in some networks there is no direct connection between the source and destination, hence multiple hops or nodes are arranged to transfer data. That passage should be secure enough so that no alteration can be done by the hacker or black node in the data sent. This also affects the security constraint of the wireless sensor network. Energy consumption by each node is very significant topic in case of wireless sensor network. Lesser the energy consumption more virtuous the network performance will be. Energy value evaluation can be done by computing the load on each node in the network. While using cryptography or any other encryption mechanism, the frequency of calculating the values like hash values, index values, integer function values etc. can be less, especially in the case of multiple hops. This increases the complexity and overhead of calculation of the values which affects the performance of the network.

IV. Conclusion

In wireless sensor network there are many algorithms that have been developed to create cipher text which is hard to decrypt. Even there are many algorithms that have been developed to securely distribute the keys between nodes inside the network so that any black node cannot join the network. We have developed an algorithm to make authentication of user most secure also we have developed a separate algorithm to make file encryption hard which cannot be decrypted by supplementary user. But still there is a limitation that is eavesdropping of file content which may be travelling in network, therefore, in future the work is required on it. Work can also be done on the safety of the network when the information is passed from source node to destination node through multiple hops active in the wireless sensor network. There is a chance of alteration of the information, if there is any unauthenticated node in the passage specified for the transmission of information. If this happens it violates the reliability parameter of the network and can give unexpected outputs. This can be prevented by securely adding the nodes in the network which should be valid and authenticated so that no black node can enter in the framework.

V. References

[1] AbdülhakimÜnlü & Albert Levi, "Two-Tier, Scalable and Highly Resilient Key Predistribution Scheme for Location-Aware Wireless Sensor Network Deployments", Springer Science, Business Media, Mobile NetwAppl-Vol.15, pp.517–529,2009.

[2] Ashok Kumar Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks", Int. Journal of Information Security,Vol. 11, pp. 189–211 , 2012.

[3] Ali Tufail,"Relay Node Deployment for a Reliable and Energy Efficient Wireless Sensor Network", Informatics Engineering and Information Science of the series Communications in Computer and Information Science, Vol. 253, pp. 449-457, 2001.

[4] Bakkiam David Deebak, "Secure and Efficient Mutual Adaptive User Authentication Scheme for Heterogeneous Wireless Sensor Networks Using Multimedia Client–Server Systems", Wireless Personal Communications: An International Journal, Vol. 87, pp. 1013-1035, 2015.

[5] G.H. Keat, A. Samsudin, Z. Zainol , "Enhance performance of secure image using wavelet compression", Int. J. Computer, Control, Quantum and Inform.,Vol. 1, pp. 165–168, 2007.

[6] Hemanta Kumar Kalita and AvijitKar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, December, 2009

[7] Kakali Chatterjee, AsokDe, Daya Gupta,"A Secure and Efficient Authentication Protocol in Wireless Sensor Network", Springer Science, Business Media New York,Vol. 81, pp. 17-37, 2014.

[8] Matteo Gaetaa,Vincenzo Loiab, Stefania Tomasiello, "Cubic B–spline fuzzy transforms for an efficient and secure compression in wireless sensor networks", Information Sciences,Vol. 339, pp. 19-30, 2015.

[9] Min, Manish Bhardwaj, Seong-Hwan Cho, Eugene Shih, Amit Sinha, Alice Wang, Anantha Chandrakasan,"Low-Power Wireless Sensor Networks Rex", IEEE Computer Society , Fourteenth International Conference ,pp. 205-210, 2001.

[10] Omar Cheikhrouhou,"Secure Group Communication in Wireless Sensor Networks: A survey", Journal of Network and Computer Applications, Vol. 61, pp. 115-132, 2015.

[11] Rudranath Mitra, Tauseef Khan, "Secure and Reliable Data Transmission in Wireless Sensor Network: A Survey", International Journal Of Computational Engineering Research, Vol. 2, pp. 748-754, May- June 2012.
[12] S. Gopikrishnan, P. Priakanth, "HSDA: hybrid communication for secure data aggregation in wireless sensor network", Springer Science, Business Media New York, Vol. 22, pp. 1061-1078,2015.
[13] Yang Yu and Viktor K. Prasanna, "Energy-Efficient Multi-Hop Packet Transmission using Modulation Scaling in Wireless Sensor Networks", Global Telecommunications Conference, IEEE Vol. 1, 2003.