IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 48-51

Secured Data Aggregation Techniques for Wireless Sensor Network

Tiwari Priti Ramesh[1], Satish Kumar[2]
Amity School of Engineering and Technology, Amity University Uttar Pradesh, Lucknow, India

Abstract: *Wireless Sensor Network (WSN) is an arrangement of numerous sensing nodes that collects and process data from surroundings and sends them through wireless/ radio links. A sensor node may contain sensitive data especially if the network is dedicated to military applications where secured transmission of data is highly recommended. This secured transmission demand privacy which is very challenging in WSN as the network is vulnerable to attack. A security approach that can be utilized for wireless sensor network is cryptography. An efficient secret key encryption and decryption along with key management can preserve the integrity of data in transmission and reception. For this approach to work, individual node is furnished with a digital key and location of each node is encrypted which is further decrypted at the sink using authentication. Authentication is done using RSA algorithm with MD-5. This paper highlights different types of security problems and attacks also how cryptographic approach can be used to preserve data integrity.*

Keywords:*WSN, Security, Attacks,Cryptography, RSA, ECC.*

I. Introduction

Wireless Sensor Networksare a diverse system that consists of many sensing nodes, processor, transceiver, actuators and power supply unit. It is the key research zone picking up its prominence because of the progression of advancements in the field of hardware and wireless correspondence.Wireless sensor systems comprise of thousands of small sensor hubs that are dispersed crosswise over expansive region [1] [2]. The sensor nodes are usually less power consuming, low manufacturing cost and self-organized wireless hubs that can sense and send the monitored data to the sink (or Base Station).These sensor hubs are application explicit and are fit for detecting the particular information and route that information to the base station at whatever point required. WSN is being used in numerous application grounds such as Environment sensing that includesforest fire detection, aquatic life under water, etc.also in health monitoring in hospitals and also in military application for detection of weapons, surveillance, etc. Many applications where WSN is being used requires secrecy of data for example in military, there can be mission sensitive information that shouldnot be easily available to the attackers as per safety concern of the nation.Securing data on the system from assaults and altering is a noteworthy point of securing transmission of information on a sensor network. This is to enhance the conditions and unwavering quality of the data the system/detecting node has. The reliance on the data is subject to the hazard related with data transmission. The more prominent the hazard related with secure transmission of data over the system, the lower the reliance on the data sent.

The secured transmission of data in WSN can demand ensuring privacy that information is conveyed to the proposed recipient(s) and kept from unapproved bug. Adjacent hubs ought to be not able pick interpretations from a hub apart from they are the proposed beneficiaries and source hub ought not spill sensor interpretations. Confidentiality of the data needs to ensured so that the sensor’s information is not accessed by any unauthorised user. The integrity of the data is equally important to assure that the data is accurate and consistent throughout the network. The data which is being delivered from source sensor node to sink or destination node must authenticate its sender and recipient inside the network and also the sender as well as the receiver should never deny about the data being sent or received by them. The data which is being transferred from source to destination node must be available throughout the network. The network should have secured data transmission and it must be accessible or retrieved whenever it is required. The data sent to the sink must be recent not the repeated information and the data must be prevented to unauthorised modification for security concern.

Sensor nodes bear some limitations in storage, processing and power supply and also, they are deployed in unsecured atmosphere which is vulnerable to many security attacks. The feebleness of wireless systems to different security risks are generally higher than the systems which transmit information by means of a wired/guided medium. This is because of the unguided medium of information transmission on wireless system. The system is inclined and vulnerable to eavesdropping. The WSN has numerous other requirements contrasted with the conventional PC systems. Direct utilization of present security methods on a customary wireless system to the WSN is very difficult because of these requirements [3]. The weakness of the immediate use of the safety efforts in WSN is the result of the attributes of the WSN in the capacity to self-organize itself, the change in topology, a network that is shared which are structured by a gathering of mobilenodes and the absence of integratedunit [5].

The limitations of resources in WSN could affect the secure transmission because some resources are required for the execution of security approach. The storage capacity of sensor nodes is very less up to few kb that results in restricting implementation of security algorithms such as cryptography. The sensor nodes mostly rely on the batteries for the power supply which can never be replaced or recharged once deployed into the area [4]. Hence, in WSN there is power limitation [6].

II. Methodology

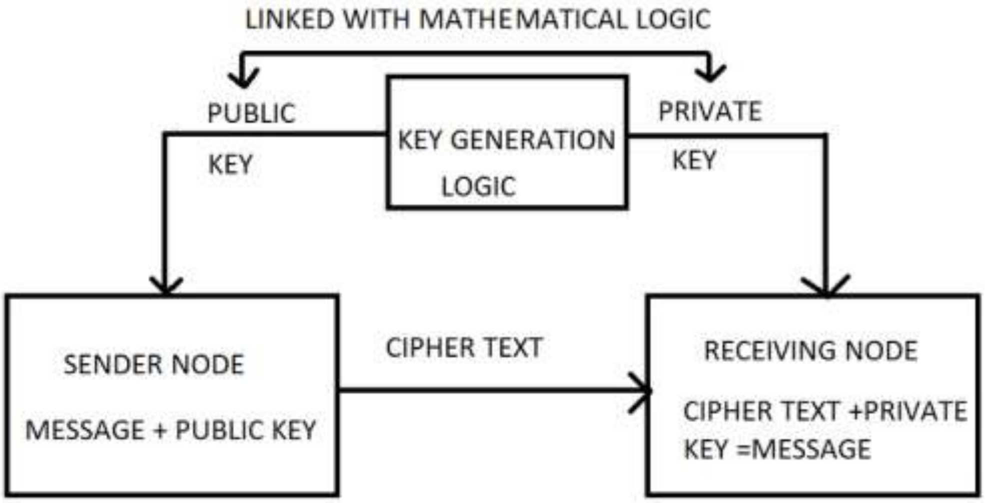

Figure 1: *Block* diagram *showing the working principle of a cryptography approach*

The various steps involved are as follows:

I. Sender Node
II. KeyGeneration Logic
III. Receiving Node

The cryptography approach cannot be directly implemented for the Wireless Sensor Networks (WSNS) as it is possible for the wired and wireless networks to enhance security because WSN is deployed heterogeneously and comprises tiny sensing nodes which has limited resources (i.e., processing, memory and battery power) [2]. Cryptography schemes demands high usage of battery power and memory storage also supplementary computation to broadcast extra bits which is required to apply cryptographic approach in WSNs. This approach in WSN increases delay, jitter and loss of packets [7]. A critical issue in the use of cryptography in WSN is the manner by which keys will be changed every now and then remembering that most sensor hubs have insignificant (or no) human cooperation. Nonetheless, preloading keys to sensor hubs before sending does not fill in as a productive answer for this test.

In meeting fundamental security necessities like confidential and integrate, Cryptography [8] approaches are frequently used. The barriers of sensor hubs can't make the notable cryptographic strategies pertinent to remote sensor systems without alterations [9].

Cryptography technique can be used by two ways:

a. Symmetric Cryptography
b. Asymmetric Cryptography

In symmetric cryptography, similar key is used to encrypt and decrypt the message from sender to receiver respectively. Whereas in asymmetric cryptography, different keys are used. The public key for encryption at the source and the secret key for decryption at the sink. Some of the techniques that are used in asymmetric key algorithm are RSA (Rivest-Shamir-Adleman) [10], ECC (Elliptic Curve Cryptography), etc.

The RSA algorithm demands two different keys, public key for encryption which is used by everyone to encode the information and the secret key to decode the same. The secret key is always resultant from the public key. The asymmetric key algorithm is widely used where secured connection is required and also it is being utilize for key management for IP security[11].RSA algorithm with MD-5 hash digest are special purpose algorithm that converts arbitrary length input message into message digest of constant length which unpredictable for attackers.The most efficient public key encryption for wireless sensor network could be ECC

[12] wherecryptography is based on two forms of predetermined fields i.e., prime fields (elliptic curves) and binary extension fields. The elliptic curve is always given by the equation [13]

$$y^2 = x^3 + ax + b$$

where a,b ϵ elliptic curve and are constant satisfying condition $4a^3 + 27b^3 \neq 0$. x,y is affine co-ordinates of elliptic curves. For finding scalar multiplication of any point on elliptic curve, elliptic curve discrete logarithm problem (ECDLP) is computationally not feasible to predict for proper constraints. This allows secured cryptographic techniques for WSN. As compared to RSA algorithm, ECC provides similar security but less computational overheads[14] [15]. ECC is not that easy to explain than that of RSA algorithm.

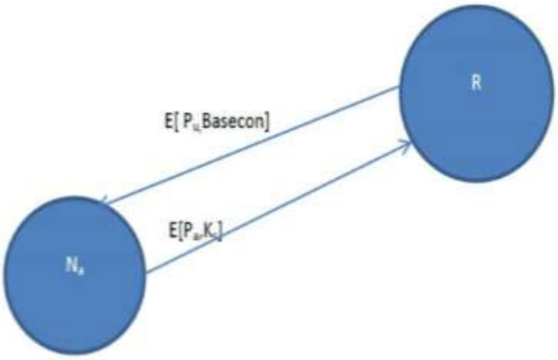

Figure 2: Illustration of confidentiality of data transmission

III. Security Attacks In Layers

LAYERS	ATTACKS	SOLUTIONS
Physical Layer	Tampering and Congestion	Spread Spectrum Communication, precise node physical suite
Data Link Layer	Collision and Exhaustion	Collision Detection techniques, TDM and Rate Limitation
Network Layer	SelectiveForwarding, Sinkhole, Sybil Attack, Wormhole and HELLO Flood	Data link layer encryption and validation, multipath steering, identity verification, authenticated broadcasting
Transport Layer	Flooding and De-synchronization	Connection-less protocols, Packet Authentication

IV. Conclusion

The WSN proceed to develop and it is becoming extensively used. In this way, the essential for security come to be imperative. On the other hand, the WSN experiences various limitations such as energy requirement, constrained computation power, memory limit, etc. Amidst different methods for giving security cryptography is more accessible.

In public key cryptography the challenging task is verification and maintaining the privacy. Different approaches are projected to overwhelmedchallenges and it can be seen that it has been achieved to great extent. It has been concluded that maintaining confidentiality and verification/authenticate the transmitted data secretly is achieved with loss of battery life. The reason behind the battery exhaustion is first node has to find the meeting point and after that it has to link a secret key to the inviting node.

Cryptography schemes demands high usage of battery power and memory storage from the sensor systems and consequently research is being carried out for creating cryptographic strategies that will help amplify these restricted resources in WSNs.

References

[1]. M. Welsh, D. Myung, M. Gaynor, and S. Moulton.(2013). Resuscitation monitoring with a wireless sensor network in Supplement to Circulation. *Journal of the American Heart Association*.

[2]. F. Akyildiz et al.(2002). A Survey on Sensor Setworks.*IEEE Commun. Mag*.40 (8), 102–114.

[3]. D. Carman, P. Krus, and B. Matt.(2010). Constraints and approaches for distributed sensor network security. *Communications Magazine*, 102-114.

[4]. A.K. Pathan, H. Lee, C. S. Hong. (2006). Security in Wireless Sensor Networks: Issues and Challenges. *ICACT*, 1043 – 1048.

[5]. K. Akkaya, and M. Younis. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*,3(3),325-349.

[6]. M. Healy, T. Newe and F. Lewis. (2007). Power management in operating systems for wireless sensor nodes. *IEEE Sensor Applications symposium*, 22-25.

[7]. M. Saleh and I. Al Khatib (2005). Throughput Analysis of WEP Security in Ad Hoc Sensor Networks. *The Second International Conference on Innovations in Information Technology*, Dubai.

[8]. W. Diffie and M. E. Hellman. (1976). New Directions in Cryptography. *IEEE Trans. Info. Theory,* 22 (6), 644-654.

[9]. J.O. Okesola, O.S. Ogunseye and O. Folorunso. (2010). An Efficient Multi-Expert Knowledge Capture Technique. *InternationalJournal of Computer Applications (IJCA),* 8(10), 6-9.

[10]. R. L. Rivest, A. Shamir, and L. Adleman.(1983). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM,* 26 (1), 96-99.

[11]. P. Ning, R. Wang, and W. Du. (2005). An efficient scheme for authenticating public keys in sensor networks. *ACM international symposium on Mobile ad hoc networking and computing*, 58-67.

[12]. A. Liu and P. Ning. (2008). TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks. *International Conference on Information Processing in Sensor Networks*, *2*(0), 245–256.

[13]. D. Hankerson, A. Menezes, and S. Vanstone. (2004). Guide to Elliptic Curve Cryptography. *Springer,* 89-93.

[14]. Anushree R. (2014). Secure Communication Using public Key Cryptography in Wireless Sensor Networks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST),* 1(4), 212-217.

[15]. N. Koblitz. (1987). Elliptic Curve Cryptosystems.*Mathematics of Computation,* 48 (0), 203-209.