Review on AES Algorithm Based Secure Data Transmission for Wireless Sensor Network

Chanderkant Sharma[1], Saurabh Anand[2]

[1]B.Tech Final Year Student, Information Technology Department, Poornima College of Engineering, Jaipur, India
2014pceitchanderkant@poornima.org
[2]Assistant. Professor, Information Technology Department, Poornima College of Engineering, Jaipur, India
Saurabhanand@poornima.org

Abstract— *Due to vast development of information technology the need of the protection of data also increases for that purpose encryption is done. The security requirements include four major aspect data confidentiality, data integrity, data authentication and data freshness. WSNs have produced enormous enthusiasm among analysts these years in view of their potential utilization in a wide assortment of uses. Sensor hubs are cheap compact gadgets with restricted handling force and vitality assets. Sensor hubs can be utilized to gather data from the earth, locally process this information and transmit the detected information back to the client. For securing that data from attack many algorithms came in existence for cryptography purpose. Be that as it may, the outstanding amongst other existing symmetric security calculation to give information security utilized these days is Advanced encryption standard (AES).*

Keywords— AES, DES, Encryption, Cryptography, Key Expansion, cipher text, WSN.

I. INTRODUCTION:

Wireless sensor networks (WSN) consists of autonomous sensor nodes attached to one or base stations. One of the main goals of wireless sensor networks is to carry reliable information from one node to another node in a network. As Wireless sensor systems keeps on developing, they wind up powerless against attacks and thus the requirement for effective security components. ID of reasonable cryptography for remote sensor systems is an imperative test because of limitation of energy, computation capability and storage resources of the sensor nodes. In this paper we have implemented Encryption algorithm AES (Advanced Encryption Standard) to provide sufficient levels of security for WSN. Advanced encryption standard has favorable position of being actualized on both hardware and software. Advanced encryption standard depends on "substitution-permutation network". It uses 10, 12, or 14 rounds in algorithm and the key size, can be 128, 192, or 256 bits depending on the number of rounds. The AES is widely used to encrypt the confidential data for security purposes.

1.1 AUTHENTICATION: The process of proving one's identity. It is another part of data security that we encounter with everyday computer usage. Just think when you log into your email, or blog account. The simple sign-in process is a form of authentication that allows you to log into applications, files, folders and even an entire computer system. Once signed in, you have different given benefits until the point when logging out. Some system will cancel a session if your machine has been idle for a certain amount of time, requiring that you prove authentication once again to re-enter. The straightforward sign-on plot is likewise executed into solid client authentication systems. Be that as it may, it expects people to login utilizing various components of authentication. Non-repudiation: In this, the recipient should know whether the sender isn't faking.For example, if suppose when one purchases something online, one should be sure that the person whom one pays is not faking.

1.2 INTEGRITY: Many a times information should be refreshed yet this must be finished by authenticated people.

1.3 Privacy/confidentiality: Ensuring that nobody can read the message aside from the expected receiver. Encryption is the way toward clouding data to make it mixed up without extraordinary learning. Encryption has been utilized to ensure correspondences for a considerable length of time, however just associations and people with an uncommon requirement for mystery had made utilization of it. In the mid-1970s, in number encryption rose up out of the sole safeguard of cryptic government organizations into people in general space, and is presently utilized as a part of securing broadly utilized frameworks, for example, Internet

online business, cell phone systems and bank programmed teller machines.

II. AES ALGORITHM

NIST started its push to build up the AES, a symmetric key encryption algorithm, and made an overall open require the calculation to succeed DES. At first 15 algorithms were chosen, which was then decreased down to 4 algorithms, RC6, Rijndael, Serpent and Two-angle, which were all iterated square figures. The four finalists were altogether resolved to be qualified as the AES. The calculation must be reasonable over an extensive variety of hardware and software systems. The calculation must be moderately basic also. After broad audit the Rijndael calculation was been the AES calculation.

Difference between AES and DES

Factors	DES	AES
Key Length	56 bits	128, 192, 256 bits
Block Size	64 bits	128, 192, 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Possible Keys	256	2128, 2192, 2256

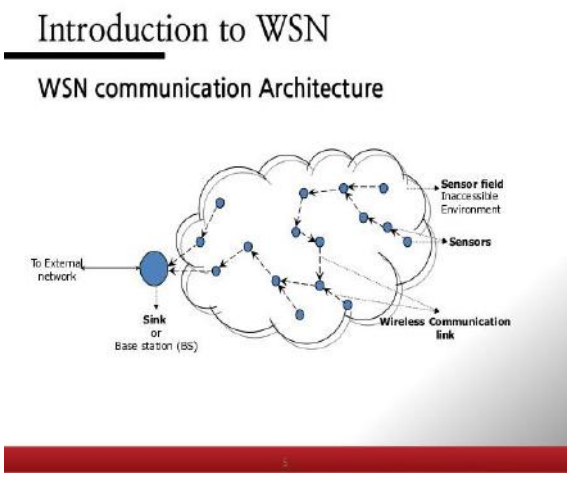
2.1 THE RIJNDAEL ALGORITHM:

For Rijndael, the length of both the square to be encoded and the encryption key are not settled. They can be autonomously indicated to 128, 192 or 256 bits. The quantity of rounds, nonetheless, differs as indicated by the key length. It can be equivalent to 10, 12 and 14 when the key length is 128bits, 192 bits and 256 bits, individually. The fundamental parts of Rijndael are basic scientific, legitimate, and table query tasks. The last is really a composite capacity of a reversal over Galois Field (GF) with a relative mapping. Such structure makes Rijndael appropriate for equipment execution.

III. WIRELESS SENSOR NETWORK:

In a typical WSN we see following network components –
Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.
Gateway or Access points – A Gateway enables communication between Host application and field devices.
Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

Security manager – The Security Manager is responsible for the generation, storage, and management of keys[5,18,19].



IV. WSN SECURITY ANALYSIS

Effortlessness in Wireless Sensor Network with asset obliged hubs makes them greatly defenseless against assortment of assaults. Aggressors can listen in on our radio transmissions, infuse bits in the channel, replay already heard bundles and some more. Securing the Remote Sensor Network needs to make the system bolster all security properties: privacy, uprightness, credibility and accessibility. Aggressors may send a scarcely any malevolent hubs with comparable equipment abilities as the honest to goodness hubs that may conspire to assault the framework helpfully. The aggressor may happen upon these malevolent hubs by buying them independently, or by "turning" a couple of honest to goodness hubs by catching them furthermore, physically overwriting their memory. Likewise, in a few cases plotting hubs may have high caliber
interchanges joins accessible for planning their assault. Sensor center points may not be change safe and if a foe deals a center point, she can remove all key material, data, and code set away on that center point. While change security might be a viable obstruction for physical node bargain for a few systems, we don't see it as a broadly

useful arrangement. To a great degree compelling alter protection tends to include critical per-unit cost, also, sensor hubs are proposed to be exceptionally economical.

4.1 AES (RIJNDAEL) OVERVIEW

Rijndael (articulated as in "rain doll" or "rhine dahl") is a piece figure outlined by Joan Daemen and Vincent Rijmen, the two cryptographers in Belgium. Rijndael can work over a variable-length piece utilizing variablelength keys; the adaptation 2 particular submitted to NIST portrays utilization of a 128-, 192-, or 256-piece key to scramble information obstructs that are 128, 192, or 256 bits in length; take note of that each of the nine mixes of key length and square length are conceivable. The calculation is composed in such a way that piece length or potentially key length can without much of a stretch be reached out in products of 32 bits and it is particularlyintended for proficient execution in equipment or programming on a scope of processors. The outline of Rijndael was unequivocally impacted by the piece figure.

V. METHODOLOGY

Data encryption is an imperative part of applying security to a wireless sensor systems. Despite the fact that transmission of information is the most energy consuming action in a remote sensor hub, it is likewise essential to choose a energy effective figure to limit energy utilization of the sensor hub. Subsequently symmetric key figure is commonly used to scramble information for transmission. Numerous block ciphers, for example, Advanced Encryption Standard (AES) utilizes various rounds of activities, for example, substitutions and linear transformations.

Secured Power Aware Routing For Wireless Sensor Security is an important factor for performance and energy efficiency in many applications. Security serves as an important role in war zone, premise protection surveillance, airports, hospitals etc. Because of the property of sensor devices, the sensor systems may effortlessly be compromised by attackers who send manufactured or altered messages. To keep data and communication systems from unlawful delivery and modification, message verification and distinguishing proof should be analyzed through certificated mechanisms. The messages transmitted from the sensor hubs over a remote sensor systems ought to be verified by the collector. The strategy of cryptography is used for this part. It is a test for the researchers to find proper cryptography for remote sensor orchestrates on account of the limitations in control efficiency, computation capability and awesome stockpiling capacities.

VI. CONCLUSION

The proposed convention has been actualized utilizing Network Simulator (NS2). The execution measurements depends on control utilization, bundle conveyance proportion. The AES Based Secure Transmission in Wireless Sensor Networks accomplishes the application determined correspondence delays at low vitality cost by powerfully adjusting transmission control and directing choices alongside consolidating a novel cryptosystem for security. To keep data and correspondence frameworks from unlawful conveyance and alteration, message confirmation and ID is inspected through guaranteed instruments. The messages transmitted from the sensor hubs over a remote sensor systems is validated by the beneficiary. The method of cryptography is utilized for this system. The sender utilizes the proposed encryption calculation to make an impression on the beneficiary, through unsecured channel, and the collector utilizes the proposed unscrambling calculation to peruse the got message. The novel cryptosystem based Secured Power Aware Routing Protocol (SPARP) upgrades Quality of Service (QoS, for example, parcel conveyance proportion, delay and diminishes the power utilization between the hubs when bundles are transmitted.

REFERENCES

[1] R. Prema and R. Rangarajan, “Secured Power Aware Routing Protocol (SPARP) for Wireless Sensor Networks”, International Journal of Computer Applications, August 2012, Volume 51, No.7, pp.13-18.

[2] R. Prema and R. Rangarajan, “Secured Power Aware and Energy Efficient Routing Protocol(SPAEERP) For Wireless Sensor Networks”, International Journal of Electronics and Communication Engineering”, International Academy of Science, Engineering and Technology, Volume 2, Issue 1, February 2013, pp.7-18.

[3] Nikolaos A. Pantazis, StefaNos A. Nikolidakis and Dimitrios D. Vergados, “Energy Efficient Routing Protocols in Wireless Sensor Networks: A Survey,” IEEE Communications Surveys & Tutorials, Second Quarter 2013, Vol. 15, No.2, pp. 551-589.

[4] S.K. Singh, M.P. Singh, and D.K. Singh, “A Survey of Energy Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks,” International Journal of Advanced Networking and Application (IJANA), 2010, Vol. 02, issue 02, pp. 570–580.