Secure Data Transmission in WSN Using 3DES with Honey Encryption

Gadkar Prathamesh S.[1], Gawali Sanket D.[2], Khalkar Yogeshwar D.[3], Narode Aniket K.[4]

[1,2,3,4] *Students, Computer Engineering Department,*
SND college of Engineering, Yeola,
Pune University
Guided by
Prof. Chandgude A. S., Computer Department, SND college of Engineering, Yeola, Pune University.

ABSTRACT

Due to the wireless nature of Sensor network, secure data transmission from one node to another node is becomes a big issue for wireless communication. The wireless network technologies are progressively gaining consideration. For different situation there are different applications are develop such as observing, control and tracing application. For these networks, camera sensor can repossess graphical statistics from an administered field, assumed that important information for different applications. Such networks have resources limitations to handling, storage, and energy and transmission bandwidth, sublime many design experiments. Due this the wireless sensor networks needs very secure communication channel to use them being in open field and broadcasting technology. In this paper to ensure the security to the various applications we will use cryptographic system. We will propose a system to securely transmit provenance for sensor data. We will introduce effective technique for provenance data verification. We will design the new system technique carefully and empirically, and the results prove its usefulness and efficient for secure provenance encoding and decoding.

Keywords- *Wireless sensor network, cryptography, 3DES, Honey Encryption.*

I. INTRODUCTION

The technology of wireless sensor node is well known technology because of its popularity. Thousands of self-organise sensor nodes are spatially distributed autonomous sensor to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. the wireless sensor network is built of "node" – from a few to several hundred or more , where each node is connected to another sensor. There is a several portion for each sensor network node: a centre antenna of radio transceiver or external antenna connection, a microcontroller, in electronic way with sensors and energy source interfacing, need a battery. The complex algorithm cannot be played over it, because nodes have not so wealthy in terms of resources. Hence security becomes a big issue in wireless sensor network.

To securely transmit [10] the various type of information over network several different algorithms cryptographic, steganography and other techniques are used. In this paper we discuss the network security fundamentals and how cryptography technique is meant for wireless sensor networks.

Cryptography [1] plays vital role for making wireless sensor network secure. There are many cryptography algorithms proposed so far: symmetric, asymmetric and hybrid. To implement a network cryptographically secure, security must be combined into every node of the network. So we need to implement security in every point of network. In WSN, cryptography algorithm should be active in nature but does not consume more memory, more power and more energy so it helps to increase the lifetime of network. But in some cases the security will be depends on the types of different application and algorithm might be particular to the application [6].

A. SECURITY REQUIREMENT IN WSN

i. Privacy **–** Privacy ensure the suppression of the information from an attacker so that any information communicated via the web should be reliable. In wireless sensor technology, the issue of privacy should have the following constraints:

a) Unless a nearest node of sensor node certified they should not allow its analyses to be recovered,
b) The encryption and decryption key delivery apparatus should be really strong,
c) In certain situation to defend against traffic examination attacks the open evidence such as sensor features, and public keys of the node should be encrypting for security reason [6].

ii. Validation **–** Validation or authentication guarantees the reliability of the information or packets by finding its genuine source. Before allowing a limited resources or information it should verifying base station cluster nodes head and other nodes. In wireless sensor network, the problem of certification should report necessity such as:

a) The node which co-operating that node will privileges to be,
b) At receiver side it should be verify that the received packet should be come from authorized sender node [1][6].

iii. Reliability **–** Reliability guarantees that message has not been lost; it gives reliable communication.. In a WSN, the truthfulness should have constraint:

a) It must be restricted that the only base station have authority that it can change the keys and web should have authority to access to the keys. Due to this, successfully check illegitimate nodes from locating information used nearby the keys and impede informs from outdoor places.
b) It should defend against an energetic, smart unauthorized node that had try and capacity to successful to costume his attack as noise [1].

iv. Accessibility – The network offered different services of resources are ensures the accessibility or they must be free if a particular sensor node required that resources. In WSN, the problems of accessibility should have some constraints such as:

a) The security of devices or networks should be available for any time; if there is any failure or system crashes, it should be avoided,
b) To transport every packets successfully to its node the central access control system mechanism is used [1] [6].

B. SECURITY THREATS

The attacker may perform various types of attacks to make wireless sensor networks unstable. The transmission medium of wireless networks are insecure because its wireless communication medium. The attacker can easily attack on wireless network.
The Security threats in WSN are broadly classified into following classes according to the attacker capability:

i. ***Inside attacks versus Outside attacks*****:** the inside attacks happen when genuine nodes of a wireless networks act as unpremeditated or illegal behaviors. Inside attacker in the sensor network is an authorized contributor who tells to create obstacle in operations or feat organizational wealth. While the external attacks, do not belong to a WSN which come from nodes. To most cryptographic things an outside attacker has no access in sensor network. External attacks may cause passive snooping on data which transmit on a web as well protect the fake data into the network due to which network resources consume and increase the possibility of denial of service (DoS) attack [2].

ii. ***Active attacks or Passive attack*****:** Passive attacks contain checking packets which exchanged within a WSN whereas active attacks involve some changes of the data stream or the making of an illegal data stream [2].

iii. ***Sensor class or laptop class attacks*:** In sensor-class attacks, an adversary attacks in a wireless network by using some nodes with similar services as that of network nodes. In laptop class attacks, an adversary can usage more powerful devices such as laptop and it can do much more damage to a network than a malicious sensor node. These devices such as laptop have a greater power, communication range, and battery backup than the network nodes [2].

II. LITERATURE SURVEY

In paper [1], study on security of wireless sensor network, in today's world wireless technology very fast developed and mostly used in many sectors. Hence, the necessity for security becomes very crucial factor. Though, the wireless network technology has some restriction such as limited battery power, processing ability, and capacity of memory storage, etc. For this constrains, many new security mechanism and technologies have been develop to overcome this challenges. There are many technologies are available to provide security against the attackers, one of the best technology is cryptography.
In paper [2], they focus on different problem in wireless sensor network. Also study on different possible attacks on WSN. In paper "Environment Based Secure Transfer of Data in Wireless Sensor Networks", converse on the security in transformation. In past few years lack of information are spread from one place to another hence it is very important that the data should transfer securely without data loss.
In paper [3], the relative study between DES, 3DES shows that the Threefold DES simply extends the key size of DES by applying the algorithm three times in progression with three different keys, hence 3DES more leading and has high performance than DES.
The paper [7], TDES is used in various cryptographic applications and wireless protocol and security layer. The encryption algorithm DES, 3DES, AES are not work better against the brute-force attack here we need to solution to avoid the brute force attack. The new encryption skill known as Honey encryption, use honey encryption the problem can be solved.

III. PROPOSED SYSTEM

The system will make use of Three-layered Data Encryption Standared (TDES) algorithm, Honey Encryption and trusted platform for enlarged security. The system provides security for application data from unofficial user. The data is secure with origin verification by providing security against malware attack. For secure discovery of malware two elements will be use, sign and verify. Both elements check the key entered by the authorised person with provenance approach.

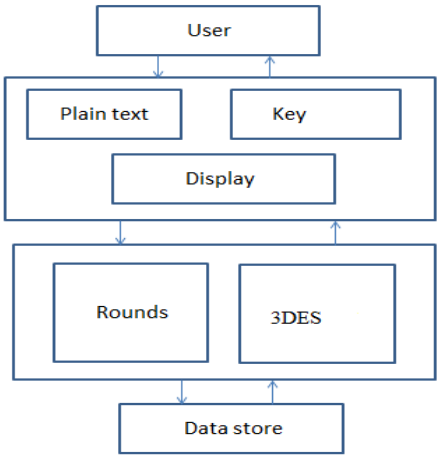

Figure 1: System Architecture

A. PROPOSED TECHNIQUES

1.1 Data Encryption Standard (DES)

DES is most broadly use encryption algorithm [4]. DES is specified in FIPS PUB 46, is a Feistel-type Substitution-Permutation Network (SPN) cipher. A U.S. encryption standard the result of a 1970s effort to produce. Using brute-force attack DES key which easily can be broken and each key is a 56 bit. A 16 cycle Feistel system is used, with an overall 56 bit key permuted into 16 48 bit sub keys, one for each cycle. The order of sub keys is reversed, which uses same algorithm. The elastic a total block size is 64 bits of each L blocks and R blocks. The L and R blocks are 32 bits each. The hash function "f", stated by the standard use called "S-boxes". It takes a 32 bit data block and one of the 48 bit sub keys as input and produces 32 bits of output. Sometimes DES is said to use a 64 bit key, but 8 of the 64 bits are used only for parity inspection, so the effective key size is 56 bits [3] [4].

The purpose of data encryption standard algorithm [4] is:

i. ***Extension (E):*** The 32 bit input expression is first extended to 48 bits by copying and rearranging partial of the bits.

ii. **Mixing key:** The stressed expression is x-or with a round key assembled by choosing 48 bits from the 56 bit top-secret key, a different choice are used in each round.

iii. ***Replacement:*** The 48 bit outcome is split into eight 6 bit words which are interchange in eight parallel 6×4 bit S boxes. All eight S boxes are dissimilar but have the special structure.

iv. ***Permutation (P):*** The resulting 32 bits are restructured rendering to a static permutation before being sent to the output. The changed R Block is then X OR with L Block and the resultant fed to the next R Block register. The genuine R Block is fed to the next L Block register. With additional 56 bit derivative of the 64 bit key, the same process is repetitive.

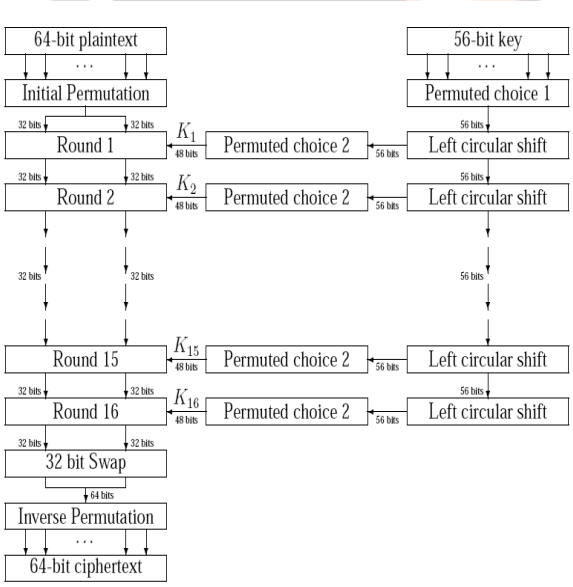

Figure 2: Data encryption Standared

1.2 Triple Data Encryption Standared

Triple DES is an upgrading of DES [3] [9]. It has 64 bit block size and 192 bits of key size. The encryption method is analogous to the one in the original DES but applied 3 times to increase the encryption level and the average safe

time. However, DES is only a 64 bit (eight characters) block cipher, an in-depth search of 255 steps on average, can retrieve the key used in the encryption, there is no reasonable way to break DES. For this reason, it is a mutual preparation to defend serious data using something more powerful than DES. Triple DES much more secure form of DES, Triple DES is just DES done 3 times with two keys used in a particular order, hence it is much safer than the plain DES [5][7].
A different of modes of TDES [7]:

i. DES-EEE3: Three DES encryptions with three different keys.
ii. DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
iii. DES-EEE2 and DES-EDE2: Same as the previous layouts excluding the first and third operations use the same.

Let EK (I) and DK (I) denote the DES encryption and decryption of I using DES key K correspondingly. Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations. The following operations [7] are:

i. TDEA encryption operation: the conversion of a 64-bit block I into a 64-bit block O that is defined as follows: O = EK3 (DK2 (EK1 (I))).
ii. TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: O = DK1(EK2(DK3(I))).

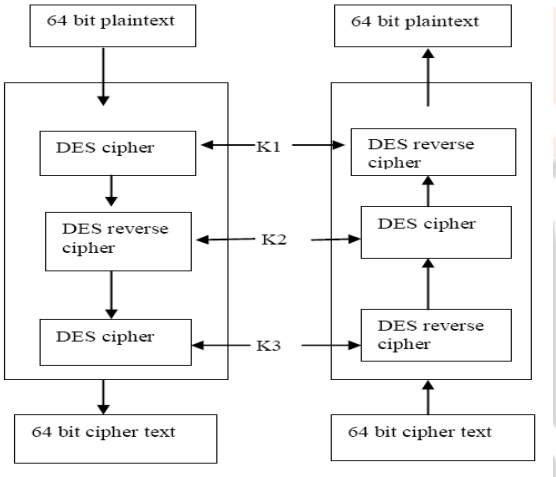

Figure 3: Triple DES

1.3 Honey Encryption

Most present encryption schemes use an n-bit key, where the security of the encryption rises with the size of the key. Although we consider these schemes secure, with sufficient computational power they are susceptible to brute-force attacks. The encrypted text using decryption through brute-force guessing of keys can be confirmed with a valid observing message output, but more importantly, an invalid-looking output as approval of an unsuccessful attempt. Honey encryption [8] offers a solution to this susceptibility for certain types of messages. An encrypted text that is honey-encrypted has the property that attempted decryptions with unlawful keys yield valid-looking output messages. Thus, attackers employing a brute-force approach gain no information from guess and checking of keys.
Juels and Ristenpart proposed this concept of honey encryption specifically in the context of passwords. After a leakage of millions of real user passwords, it was observed that a significant number of people used weak, easily-predictable, and repetitive passwords. Password-based encryption and hashing methods both carry the same vulnerabilities to brute-force guesstimating attacks due to the probability of user made passwords. By using honey encryption instead of old PBE, the certainty of an attacker for successful decryption of a password is damaged [8].

The main revolution of the honey encryption scheme is the distribution-transforming encoder, which plans the space of plain-text messages to a seed space of n-bit strings. The DTE takes into account a possibility distribution of the message space and assigns a corresponding ratio of bit strings to the message. The insight lies in the fact that all potential decryptions, irrespective of accuracy, map to some message and since possible decryptions are assigned via the expected possibility distribution, the attacker gains no information. Constructing a suitable DTE for various applications of honey encryption requires an understanding of the message space distribution [8].

IV. CONCLUSION

Trust in WSNs is still challenging field due to its dynamic nature. However it is a very rewarding area as most of the WSN applications are deployed in hostile environments such as military fields. The TDES algorithm can provide high security for transformation of data. The TDES algorithm provides high-speed performance with very compact hardware implementation. TDES has better performance than DES. The electronic industry uses Triple DES to protect user content and system data. As well secrets key such as passwords is needed to be secured in computer systems for many years. Their use in encryption leaves resources vulnerable to offline attack. Honey encryption can offer valuable additional protection in such scenarios. Honey encryption provides security against Brute-Force attack.

REFERENCES

[1]. Salmin Sultana,Gabriel Ghinita, *Member, IEEE,* Elisa Bertino, *Fellow, IEEE,* and Mohamed Shehab, *Member, IEEE "*A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks*",* IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTIN VOL. 6, NO. 1, JANUARY 2015

[2]. Mahfuzulhoq Chowdhury1, Md Fazlul Kader2 and Asaduzzaman1 "Security Issues in Wireless Sensor Networks: A Survey", International Journal of Future Generation Communication and Networking Vol.6, No.5 (2013), pp.97-116

[3]. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AESwithin Nine Factors", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[4]. Prashanti.G, Deepthi.S, Sandhya Rani.K "A Novel Approach for Data Encryption Standard Algorithm", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013

[5]. RIMPI DEBNATH, PRIYANKA AGRAWAL, GEETANJALI VAISHNAV "DES, AES AND TRIPLE DES: SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014

[6]. Mrs. B. Vidhya1, Mrs. Mary Joseph2, Mr. D. Rajini Girinath3, Ms. A. Malathi4 "ENVIRONMENT BASED SECURE TRANSFER OF DATA IN WIRELESS SENSOR NETWORKS", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015

[7]. Mandeep Singh, Narula Simarpreet Singh "Implementation of Triple Data Encryption Standard using Verilog", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 ISSN: 2277 128X

[8]. Ari Juels, Thomas Ristenpart "Honey Encryption: Security Beyond the Brute-Force Bound", University of Wisconsin, January 29, 2014Version 1.1

[9]. Amit Dhir "Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs",White Paper: Spartan-II FPGAs, WP115 (v1.0) March 9, 2000

[10]. Gulustan Dogan and Ted Brown City University of New York, Graduate Center, 365 5th Ave, New York, NY 10016 "A Survey of Provenance Leveraged Trust in Wireless Sensor Networks", Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.5, No.2, 2014

[11]. Sumit Chaudhary, Neha Singh, Avinav Pathak and A.K Vatsa IIMT Institute of Engineering & Technology, Meerut , U.P, India, "Energy Efficient Techniques for Data aggregation and collection in WSN", International Journal of Computer Science, Engineering and Applications (IJCSEA)Vol.2,No.4,August 2012.

BIOGRAPHIES

Gadkar Prathamesh S. pursuing the B.E. degree in Computer Engg. From S.N.D COE & RC, Yeola in 2015.

Gawali Sanket D. pursuing the B.E. degree in Computer Engg. From S.N.D COE & RC, Yeola in 2015.

Khalkar Yogeshwar D. pursuing the B.E. degree in Computer Engg. From S.N.D COE & RC, Yeola in 2015.

Narode Aniket K. pursuing the B.E. degree in Computer Engg. From S.N.D COE & RC, Yeola in 2015.