N-Column Authentication Key Building with Multi-Round Cryptography for Higher Level of Security in 4G networks

Kanica
Dept. of CSE
CGCC-COE,Lnadran

Anuj Kumar Gupta
Dept. of CSE
CGCC-COE,Lnadran

Abstract - The 4G networks are rising their popularity across the cellular networks are every year more and more users are joining the 4G networks. The 4G networks are high-speed cellular and internet networks, which includes the high bandwidth ability for the data transfer, call data handling and other such data transfer events. The high bandwidth invites the various hacking attempts over the network for the stealing of the higher bandwidth. Also the hacking attempts are made over the 4G network for the snooping of the voice data from the active channels. Hence the 4G networks are in critical need of the security imposition using the authentication or encryption techniques. The existing 4G security model offers four-message based authentication model for LTE authentication on each round. The existing model utilizes the elliptic curve cryptography over the key build from the two values (or two-columns) mechanisms for the key table generation. The existing model does not protect against the cryptanalysis attacks because of weak cryptography and higher time complexity because it is computationally complex. The proposed model offers the two-message based authentication model for LTE authentication on each round using the robust AES encryption for the key data hiding. The proposed model offers the more flexible N-column pattern to build the stronger keys with simple and robust authentication model with low computationally complex operations. The proposed model has been tested under various scenarios for the experimental assessment of the performance. The proposed model has been outperformed the existing model on the basis of the performance parameters of time complexity and overhead.

I. INTRODUCTION

A wireless sensor network is made up of nodes and these nodes vary in range according to the area in which they are located. The nodes may be few to hundreds or several thousands. Each node is connected to one sensor or sometimes to several sensors. Although, each sensor network node consists of many parts that are a Microcontroller ,a Radio Transceiver which may be connected to an external antenna or may have an internal aantenna connection and an electronic circuit that is used to interface with sensors and energy source and it is usually the battery to harvest the energy. The size and cost of sensor network nodes are variable that results in corresponding constraints on resources such as computational speed, storage capacity, energy, and processing and communication bandwidth.

The WSN has a very huge equipped region and it is used in different areas like monitoring of environmental factors, controlling humidity and temperature, controlling traffic, monitoring of individual body organs and so forth. The figure depicts a state of WSNs in medical field where the patients are being monitored whether at homes, in hospitals or in open-air where they are doing their daily activities. And this monitored data are then sent to the wellbeing professionals passing through the internet.

A number of applications need security while transporting the information via internet, for instance the sensor nodes are entrenched in human body and reports to the health professional. As the health experts believe that authentication and access control is must during the transmission.

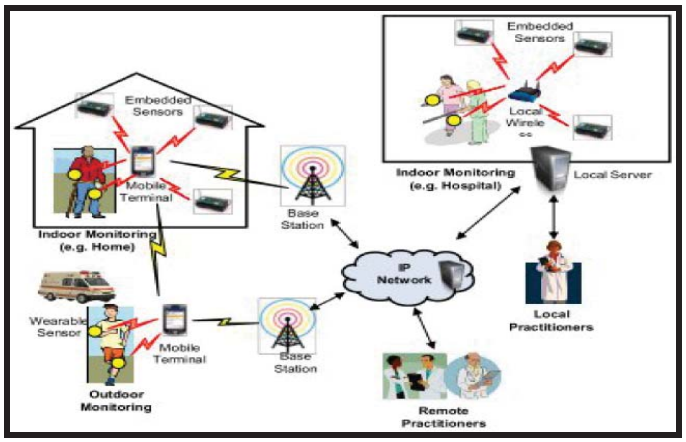


Figure 1.1: Scenario of Wireless sensor network

.Apart from the health area, other fields like industry, military applications, environmental applications, structural applications also need security during the transmission of information through the internet. So, security is the main concern in wireless sensor network.

1.1.1 Wireless Sensor Network

A wireless sensor network (WSN) is a collection of large number of devices and these devices are known as sensor nodes, which are small in size and these are battery powered. The sensor nodes are equipped with one or more sensors, small amount of storage capacity, central processing with limited computational capabilities, battery power supply and radio communication. The nodes communicate with each other through wireless network as they do not depend on any pre-deployed architecture and these sensor nodes use the radio signals to communicate with each other. The power of each sensor device is provided by battery. The sensor devices are collaborate with each other in order to perform sensing, communication and processing that is sharing and transceive data and these devices are act independently in order to operate in an autonomous and distributed manner. The sensor nodes monitor the physical and environmental conditions like temperature, pressure, humidity, pollutants, sound etc and pass their data via network to the main location where the data can be observed and analyzed.

The sensor network devices are created by a computational part and sensing part. The computational part is in charge to store and transmit data and sensing part is created by more than one sensor. Basically, two formats are used to made sensor devices that are Frequency Shift Keyed (FSK) which is working at 433 and 868-915 MHz and Direct Sequence Spread Spectrum (DSSS) which is working at 2.4 GHz. The radio range varies from 10 to 100 meters. The transmission rates could be 19.2 kbps to 240 kbps due to the configuration of antenna. The matter of energy is the most significant concern as the sensor nodes are battery driven. In these days, available sensor node in the market are IRIS, MICAz, LOTUS and Mica2.

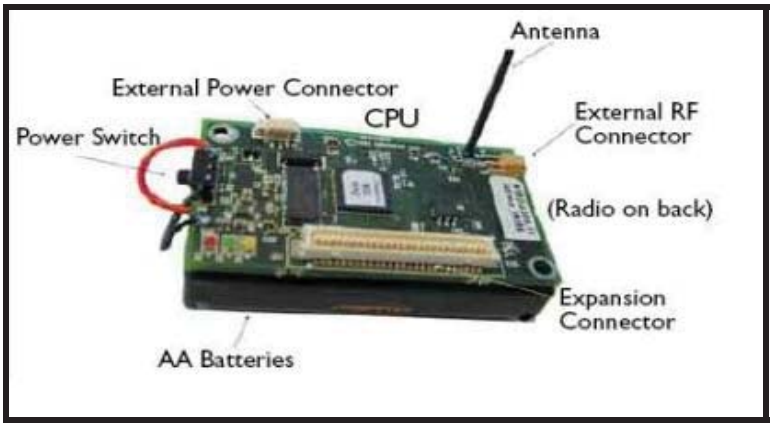


Figure 1.2: configuration of sensor

The environment, in which these sensor devices are deployed, may be controlled or uncontrolled. If the environment is controlled then these nodes are manually established to achieve the deployment but these types

of deployments are not much feasible or can be possible if the numbers of nodes are in large amount. In contrast, if the environment is uncontrolled, as there is very large WSN, then deployment is achieved by randomly scattering the nodes to the target locations. These sensor nodes are distributed in specified areas and are able collaborate data and then provide information about the environment in which they are deployed, in order to provide clear observations.

1.2 Literature Review

1. Alagheband and Aref (2012) proposed a dynamic key management infrastructure for the mixed WSNs which were based on elliptic curve cryptography and between the clusters and base stations with the help of sign cryption technique instead of doing encryption with signature, sensor node versatility, verification to save sensor node traded off in the clusters. The proposed plan had system versatility and sensor node portability particularly in fluid situations. Both occasional verification and another enrollment mechanism were proposed through counteractive action of sensor node traded off. The creators investigated a portion of more influential varied WSN key administration plans and contrasted them with the proposed plan. After contrasting the proposed plan with more determined progressed mixed WSN key management conspires, the proposed system separately turned out to be better as far as correspondence, calculation and key storage. The scheme was proposed after observing the various types of insecurities among the wireless sensor network.

2. Alcaraz et.al (2012) proposed a tool named SenseKey tool which was used by network designers to choose a better key management protocol that was efficient to provide security to their sensor hubs. Because of the major role of Key Management Schemes to identify security measures that is why it was important to select best key protocol for the entire network. Also, it tackled the problems related to up-to-date research on key management scheme for non-hierarchical sensor networks, only to provide solutions in different wireless sensor network application for creating link layer keys.

3. Bawa et.al (2012) presented a random key distribution scheme with the help of NchooseK algorithm in WSNs as they observed that key management is very difficult to achieve in sensor networks. By random key distribution they were able to reduce the limitations of pre-shared key scheme. The environment of WSN faced many confines so to reduce them it was burning used to supervise memory which was consumed. Nchoosek algorithm provided network connectivity to made network more consistent and suggested a scalable solution in each node. There was no need to keep key material of whole network. The proposed scheme improved the packet delivery and condensed the rate of dropped packets. By dropping the traffic over network, performance of entire network had increased.

4. Bechkit et.al (2012) proposed a new highly scalable key establishment scheme for WSN. For this, they used unitals design theory and showed the mapping from unitals to pairwise key establishment so that high n/w scalability be achieved despite the fact that the chance of key sharing is corrupted. After that, they proposed an enhanced unital-based pre-distribution approach that provided high network scalability and good chance of key sharing. Also, carried out logical calculations and demanding replications to compare their solution with existed solutions as to improve the scalability of network after providing better performances. The solutions they provided significantly reduced the storage capacity at the same network size.

5. Jayanthi and Mukunthan (2012) proposed a stable link clustering algorithm (SLCA) that provided versatility of joins and adjoining nodes for long time. SLCA was in light of the highest connectivity criterion with topology solidness advancements. While secrecy related issues had been widely concentrated on in-installment based framework, for example, e-money and shared (PPP) framework, little exertion had been dedicated to remote cross section systems. Security construction modeling chiefly comprising of ticket based conventions, which determined the clashing security prerequisites of unqualified anonymity for the legit clients. By the use of SLCA architecture, the proposed work established efficiency as well as desired sought among security targets that were confirmation, confidentiality, information trustworthiness and non-repudiation.

1.2 Algorithm

Key Exchange Mechanism

1.2.1 Key Generation Policy: Key generation policy under the proposed model is using the following mathematical algorithmic flow to populate the key table which is saved and being exchanged between the user nodes in the working cluster.

Algorithm : Randomized Function To Generate Algorithm

1 .First, initialize the random number generator to make the results in this example repeatable.

2. Create a radii value for each point in the sphere. These values are in the open interval, $(0,3)$, but are not uniformly distributed. The values have been created using the mathematic equation:

$$f(x) = 3 * \int_{1}^{1000000} random * \frac{1}{3}$$

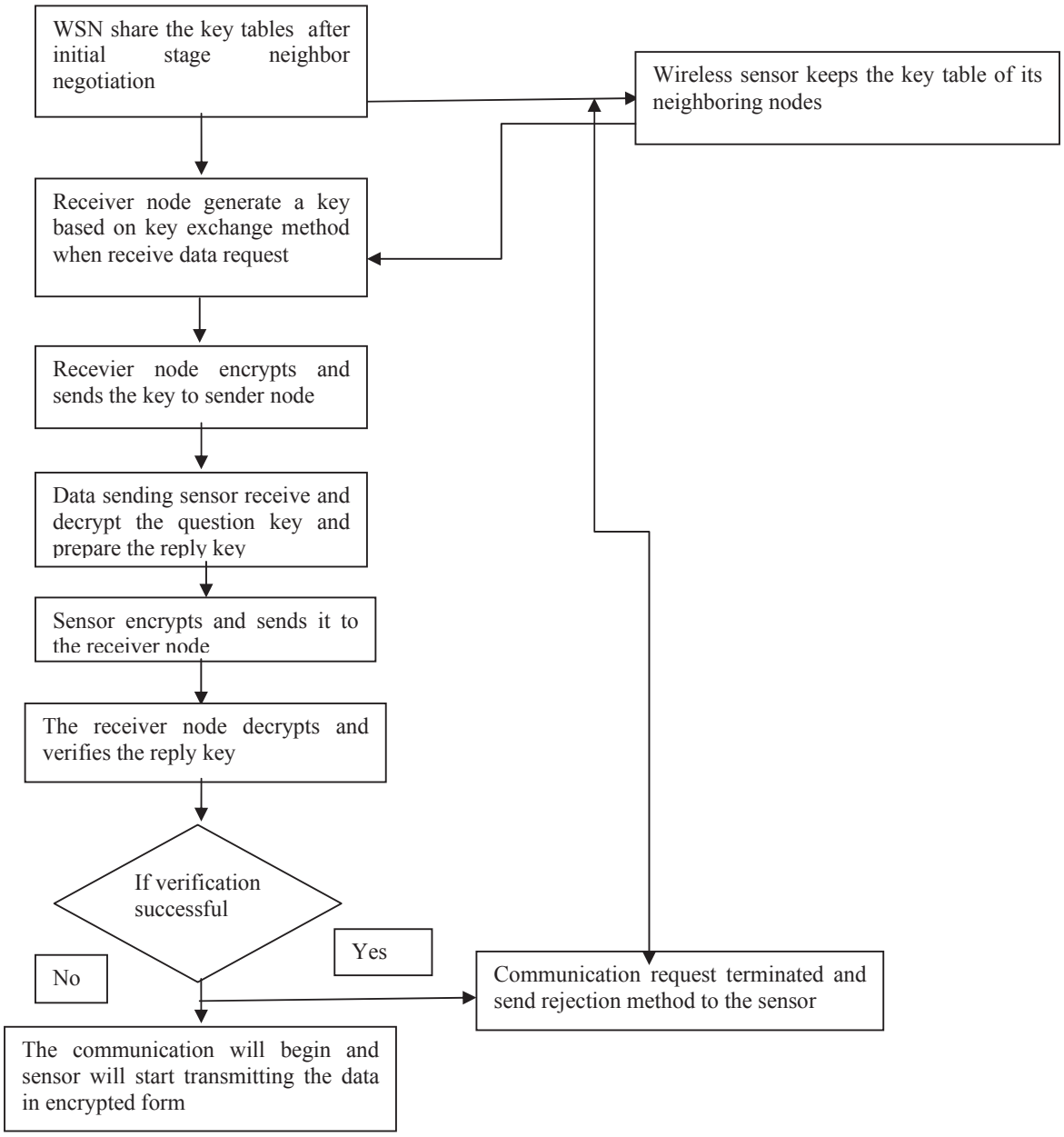
3. Randomly select and concatenate the coordinates or values to create the OTP.
4. Return OTP

1.2.2 Key Management Policy: To protect the communication we are proposing a novel key exchange methods based upon the randomized key generation and management policy as the major improvement for the diffie-hellman scheme. Our scheme does not rely upon the key reversal or re-computational process, but is robust and rigid in nature, which does not allow any of the key guessing attacks. Such attacks do not let the sensor device to become hostile to the hackers and do not expose any information to the hackers. Our key scheme has been described in detailed below:

Algorithm : Proposed WSN based Multi Level Authentication Protocool

1. The sensor nodes powers up
2. The sensor node X initiates the data propagation process
3. The sensor node X sends data channel request to sensor nodes
4. The sensor node Y sends a verification key
5. The sensor node X reply with the corresponding verification acknowledgement key.
6. The sensor node Y verifies the authentication key my matching the authentication against the verification key
7. If key verification successful
    a. The sensor node X is updated with an acknowledgement to send the data and start the time counter for secure channel period
8. Else
    a. The sensor node X is denied the data connection.
9. When the secure channel period time counter expires
    a. The node Y resends the verification key again to the sensor node X
    b. The sensor node X reply with the corresponding verification acknowledgement key
    c. The sensor node Y verifies the authentication key by matching the authentication against the verification key
    d. If key verification successful
        i. The sensor node X is updated with an acknowledgement to send the data and start the time counter for secure channel period
    e. Else
        i. The sensor node X is denied the data connection.
10. Repeat the step 3 when data communication is running.

1.3 Flow chart



II. CONCLUSION

The proposed model has been described for the sensor network security by offering the robust key management scheme. The proposed key management scheme has been designed to add the minimum possible overhead upon the sensor network by exchange the minimum possible authentication packets containing the secure key information to authentication the communication channel between the two nodes. The proposed model has been developed and tested with the scenarios of 100 nodes. The results have been obtained in the form of energy consumption and communication efficiency. An ideal key management protocol should not add the over-burdened communication overhead which can be measured by the communication efficiency. The efficiency of the key management protocol can be measured from the energy consumption which has been caused due to the communication overhead, and also acts as the perfect measure for the sensor network efficiency. The proposed model results have been obtained in the form of communication overhead and energy consumption. The proposed model has been found efficient than the existing models on the basis of result analysis performed on the results obtained from the proposed and existing model. The experimental results have signified the improvement in the performance of the sensor network while using the proposed key management scheme

REFERENCES

[1] Stefan Craciun, Gongyu Wang, Alan D. George, Herman Lam, Jose C. Principe, "A Scalable RC Architecture for Mean-Shift Clustering", ASAP, pp. 370-374, IEEE 2013.

[2] Shivani Agarwal, Lionel SujayVailshery, MadhumithaJaganmohan and Harini Nagendra, "Mapping Urban Tree Species Using Very High Resolution Satellite Imagery: Comparing Pixel-Based and Object-Based Approaches", ISPRS, pp. 220-236, IEEE, 2013.

[3] Nagendra, H.; Lucas, R.; Honrado, J.P.; Jongman, R.H.G.; Tarantino, C.; Adamo, M.; Mairota, P. Remote sensing for conservation monitoring: Assessing protected areas, habitat extent, habitat condition, species diversity and threats. *Ecol. Indic.* **2012**, doi:10.1016/j.ecolind.2012.09.014.

[4] Boyd, D.S.; Foody, G.M. An overview of recent remote sensing and GIS based research in ecological informatics. *Ecol. Inform.* **2011**, *6*, 25–36.

[5] Gairola, S.; Proches, S.; Rocchini, D. High-resolution satellite remote sensing: A new frontier for biodiversity exploration in Indian Himalayan forests. *Int. J. Remote Sens.* **2012**, *34*, 2006–2022.

[6] Nagendra, H.; Rocchini, D. High resolution satellite imagery for tropical biodiversity studies: The devil is in the detail. *Biodivers. Conserv.* **2008**, *17*, 3431–3442.

[7] Wang, K.; Franklin, E.S.; Guo, X.; Cattet, M. Remote sensing of ecology, biodiversity and conservation: A review from the perspective of remote sensing specialists. *Sensors* **2010**, *10*, 9647–9667.

[8] Benz, U.C.; Hofmann, P.; Willhauck, G.; Lingenfelder, I.; Heynen, M. Multiresolution, object oriented fuzzy analysis of remote sensing data for GIS-ready information. *ISPRS J. Photogramm.* **2004**, *58*, 239–258.

[9] Blaschke, T. Object based image analysis for remote sensing. *ISPRS J. Photogrammm.* **2010**, *62*, 2–16.

[10] Gibbes, C.; Adhikari, S.; Rostant, L.; Southworth, J.; Qiu, Y. Application of object based classification and high resolution satellite imagery for savanna ecosystem analysis. *Remote Sens.* **2010**, *2*, 2748–2772.

[11] Dr. Anuj Kumar Gupta; Kanica "Areview on multilayer security architectures/models for 4G/LTE networks" IJLTET 2016 – 449.