ACTIVE DYNAMIC KEY FOR SECURE DATA TRANSFER IN WIRELESS SENSOR NETWORK

Vikkram R¹, Rajeshkumar G², Sadesh S³

¹Assistant Professor, Department of Information Technology, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.

²Associate Professor, Department of Information Technology, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.

³Associate Professor, Department of Information Technology, Velalar College of Engineering & Technology, Erode, Tamilnadu, India.

¹vikkramg@gmail.com, ²grajesh.grk@gmail.com, ³sadesh_vcet@yahoo.com

Abstract

The day to day life billions of data are transferred across the internet using millions of devices. These transferred data are theft or falsifying the original content by the intermediates when transferred from source to destination. So that data is transferred in a secure manner it does not theft or replicate. In the Virtual active key-based encryption a new idea of one-time active dynamic key is used (i.e.) while information transferred between the source and destination the original data is encoded with this key and the algorithm. A Secure undisclosed or secret key is created and applied to single packet and the different one-time active key is applied for consecutive packets, which is a protected communication context, the information to be sent is encoded with the Advanced Encryption Standard (AES) algorithm. The in-between nodes authenticate the acknowledged data packets if the received packet is untruthful or malicious data transmitted by any intruder such packets are noticed and removed or else the data is transferred to the succeeding node. In this Encryption method, there are two modes of operations that are carried out they are VABEK-I and VABEK-II [VABEK-Virtual Active Based Encryption Keying]. In VABEK-I every node observe their adjacent node and in VABEK-II every node arbitrarily chooses the nodes and track them. Thus, the two methods check all units and check those data packets if the data is a malicious one its dropped.

Keywords: WSN, One-time dynamic active key, VABEK-I, VABEK-II, AES

I. Introduction

In the communication between the wireless sensor networks, the malicious outsider sends the duplicate packets along with the significant packets from one source to destination. For that, we have to identify the false packets and drop them. Successful completion of this project solved the intruding packets.
The massive evolution of communication proposals only huge benefits in rapports of secure interchange of data. There are Two significant methods are used in Wireless sensor networks: fixed and active. In the fixed key method, the key creation and the circulation are held static. That means the devices possess a key that lasts for a long time and is loaded prior or soon subsequent communication is formed and placed. The active dynamic key method accomplish rekeying ie performs setting function occasionally bases on request as need by the WSN. VABEK-[Virtual Active Based Encryption Keying] structure is based on two operational modes. They are VABEK-I and VABEK-II. The VABEK-I nodes comprises of one leap. VABEK-II comprises entirely of moving nodes. The Performance of the VABEK's feasibility and performance can be analyzed in two different ways.

Those are the Rational Procedure and duplications. This two are constructed on the response component as well as destination. The through put also analyzed when routing the packets from one node to another. This checks the through put of the individual nodes. The transmission path is stable through the delivery. VABEK-I is secured one because of the crucial data is ciphered using disposition via Advanced Encryption Standard. Each data packet uses different keys. The transmitted packet size is increased to avoid redundant data.

This Technique has the capacity to transfer 64-bit data compared to other encryption algorithms they have a capacity to transfer 40 bits of data. The key size of 8 to 10 digits is generated and applied to the whole message to provide high security. The secret component and data broadcast are used in sensor. The AES encryption is used to alter the virtual active key of the sensor.

II. Overview of WSN

Wireless Sensor Network plays the key role in day to day activities comprises of geographically expanded independent sensors to observe tangible and usual calamities, such as noise, pressure, and temperature, etc. and transfer easily transfer the data through across the network. It was initially used in military purposes like battleground monitoring. Today such WSN is used in consumer as well as industrial applications. The wireless sensor network is made of few nodes range small numbers to few hundreds even to millions, where every node has single or multiple sensors. Each sensor consists of a radio transmitter as well as receiver, microcontroller and an inbuild antenna or external antenna with an interface with sensors by an electronic circuit. A battery is attached in the form of active yield. The size and charge of the sensor device are based on the restraints on the sources. The WSN topology is different from a multi-hop mesh to the star network based on the environment where the network is deployed. The communication is achieved in every device in the network through routing or flooding.

III. System Platform

Bundled Software

The uncommon basis of wireless sensor network devices is active, which controls the life duration of the WSN. Every WSN are purpose to place in numerous numbers of mixed environments, with corresponding distance and
critical sections, where as in ad-hoc networks are key module. for these protocols and procedures are required to report the subsequent problems:

- Era extension
- Firmness and fault forbearance
- Self-structure

**Era Extension**

To use the sensing device for a lifetime the radio power supply is shut down when the device is not in use, because the utilization of power in the sensors will dry out the battery when it is idle.

**Firmness and Fault Forbearance**

The fault tolerance is the main issue that WSN experience problems by various circumstances such as the depletion of power, environmental issues, interferences of radio, collision, and dislocation of sensors. To overcome this the node will send an alert message if it encounters any of the above issues so that it can be rectified as soon as possible.

**Self-Structure**

Each node is aware of its neighboring nodes so that it can calculate the path of transmission and reroute the data to the end point via the shortness path it takes with minimum amount of time to reach.

**Hardware**

The biggest and main challenges in wireless sensors network is to produce the device at a small size and low cost. Nowadays there are numerous companies producing wireless sensor network hardware and in the late 1970s, the commercial environments can be compared with the modern one. Many nodes are in the process of study and in the developing stage, mainly the software used in them. In many environments, the WSN connects with LAN or WAN during the gateway and these sensors achieve the data transfer by the use of low power consumption methods.

**IV. Related Work**

The main disadvantages in the existing system are it uses the RC4 algorithm, where safety is low and data is interconnected up to 40 bits. An Ancient and simple method is followed in it, iostream cipher methodology is used to encode the rivulet of data. A single WSN is comprises of a huge number of tiny sensor devices, which are organized closely. The place or location of the sensor devices need not be guessed or engineered.

This permits us to position every device randomly over remote terrains and disaster-affected areas for relief operations. This refers to each sensor network must have protocols and algorithms to organize themselves. These nodes are fitted along with the on-board processor that makes them work in a cooperative manner.

The sensor nodes placed in the region collect the raw data from the surroundings, instead of sending as it is, each node carries out some simple computations on the
collected raw data and make the data as partially processed before it sends the data to another node or server. Recognizing the received computed data the other nodes as well as the server passes the data or compute it further to get the acquired results.

Although many algorithms and protocols were projected for ad-hoc networks they are unsuitable for the necessities and the unique structures of sensor network. The main and significant limitations of the sensor devices is its power consumption. Therefore, the companies which manufacture the sensor nodes focus mainly on power conservation by aiming to get high quality of service.

V. Projected System

The Entire Development focuses mainly on the keying procedure of Wireless Sensor Networks. The foremost target of the WSN's to check the data packets and identify the false packets and discard them. As an alternative of implementing with RC4 algorithms the projected system uses a strong AES algorithm. Thus, it makes a few advantages when compared to the existing system. The chunk of data is encoded with block-cipher method, and it has the capability to send 8 bytes of data and in the future, the data size may be increased depending upon the usage of the data. Based on this high encryption method the entire data transfer is fully protected.

VI. Operations

The VABEK comprises four operational methods they are
1. Virtual active dynamic based key segment.
2. Data Encryption.
3. Data transceiver segment
4. Performance scrutiny segment

Virtual Active Dynamic based Key Segment

In this segment, the creation of new active keys is made out using the keying process and this contradict to the other keying schemes. It does not share any other information to generate keys. The keys are endured based on the virtual activeness of the sensor and it is calculated in the sensor nodes. Each key is feed to the successive nodes on the entire network.

Data Encryption

The VABEK uses the simple encryption technique, by processing the dissimilarity bits in the packet dynamically and creates dissimilarity code is generated using the AES technique. The VABEK is constructed elastically so that in future custom encryption mechanisms or stronger mechanisms can be adopted.

Data Transceiver Segment

This segment performs the process of transferring and reception encrypted data along with the route to reach the destination. Each sender will get the
response from the corresponding reception side to confirm the distribution of the packets.

**Performance analysis Segment**

In the segment, the false packets which are routed to the network by the external malicious outsider are identified and the false packets are discarded from the network. It also keeps track of the routing path of the packets to be transferred from source to destination. So that the packets will find the optimal path to reach the desired destination. And these events are generated as reports so that the sensor node can analyze the network performance.

**VII. Architecture**

The architecture of this proposed system uses the concept of AES algorithm.

![Architecture of Active dynamic key management](image)

**Fig.1: Architecture of Active dynamic key management**

The system works as follows, A dynamic key is generated in the source station that is a one-time active dynamic key for a single packet and consecutive different keys are generated for remaining data packets. The original content is encrypted with the Advanced Encryption Standard algorithm with the secure surreptitious key (active key). Then the Encoded data is transferred to the sensor devices. On the sensor the data are verified by decryption technique and authenticated whether the concern packets are from original source or from the malicious outsider. If the packets are identified as false, those are dropped from the network. Otherwise, it is transmitted to the mobile destination or the receiver.
VIII. Algorithm

1. Cipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)]
2. begin
3. byte state[4,Nb]
4. State = in
5. AddRoundKey (state, w)
6. for round = 1 step 1 to Nr-1
7. SubBytes(state)
8. ShiftRows(state)
9. MixColumns(state)
10. AddRoundKey(state, w ROUND*Nb)
11. end for
12. SubBytes(state)
13. ShiftRows(state)
14. AddRoundKey(state, w ROUND*Nb)
15. out = state
16. end

The AES technique used here is a substitution of Rijndael that has a block size of 16 byte and its input sizes are 16, 24 and 32 bytes. The main difference between the Rijndael technique is the key sizes may be multiple of 4 bytes with the least of 16 bytes and a maximum of 32 bytes.

Whereas AES works on the matrix format of 4x4 bytes. Most of these AES calculations are done with finite fields. It is fast in both hardware as well as software environment. The Input parameter used for the AES requires a number of rapidly changing rounds and these rounds modify the input i.e. the original data into the output i.e. encrypted ciphertext. Each round has various processing steps with four stages depends on the input. For deciphering the encrypted message to plaintext, a serious of rounds are made by applying with the same key.

IX. Illustration of the Algorithm

Key Extension

Circular key are extracted from the crypto active key by using the Rijndael's plan. For Advanced Encryption Standard128-bit circular block of keys for every round in addition to one.

Initial Round

The position of each byte is shared with the circular key block by performing bitwise XOR.

Rounds

(a)Sub-Bits: Each bit is substituted with another set of bits that are generated by non-linear substitution method as per the lookup table.
(b) **Row Shifting:** Each row is shifted cyclically for a certain number of times as per the switch step.

(c) **Mixing Columns:** Mix the columns of a matrix and combine the bytes of each column.

(d) **Add Circular Key.**

Last Round-sub bits

- shifting of rows
- add circular key

**X. Conclusion**

The paper explains the idea of using One-time active dynamic keys for one packet and different dynamic keys for different data packets. This secures the data from attacking by malicious programmers or hackers. It also gives the secure packet through engineering dissimilar keys for different packets at various times. It also shows the transmission path to be used among the nodes so that it can use the optimized path for effective data transfer. This makes the user send the data in a fully secure manner

**References**

I. Abd-alghafar, I.,Abdullah, B., Salama, G. I., Abd-alhafez, A. Performance evaluation of a genetic algorithm-based approach to network intrusion detection system Proceedings of the International Conference on Aerospace Sciences and Aviation Technology 2009 Cairo.

II. Breveglieri, L., Macchetti, M., Atasu, K. Efficient AES implementations for ARM based platforms. In: Symposium on Applied Computing, pp. 841–845. ACM, New York (2004)

III. Chen, H.-H, Liu, H, Khanna, R,... Reduced complexity intrusion detection in sensor networks using genetic algorithm Proceedings of the IEEE International Conference on Communications June 2009 152-s2.0-7044948512210.1109/ICC.2009.5199399

IV. Eboka, A. O, Aghware, F. O, Ojugo, A. A., Okonta, O. E., Yoro, R. E., Genetic algorithm rule-based intrusion detection system (GAIDS) Journal of Emerging Trends in Computing and Information Sciences 20123811821194.

Copyright reserved © J. Mech. Cont.& Math. Sci.
*
Vikkram R et al

180
V. F. Zao, J. Liu, Y. Zhang, and, “Robust distributed node localization with error management,” in Proceeding of the 7th ACM International Symposium on Mobile Ad-Hoc Networking and Computing 2006, pp. 250–261, Florence, Italy, May 2006.

VI. J. Leonard, D. Moore, D. Rus, and S. Teller, “Robust distributed network localization with noisy range measurements,” in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems 2004, pp. 50–61, November 2004.

VII. K. Gaj and P. Chodowiec, Very compact FPGA implementation of the AES algorithm. 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2003), pages 319-333, Germany, Sept. 8-10, 2003.

VIII. Lade, S. Dhak, B. S. An evolutionary approach to intrusion detection system using genetic algorithm International Journal of Emerging Technology and Advanced Engineering201222632637.

IX. M. Benaissa. And T. Good AES on FPGA from the fastest to the smallest. 7th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), pages 427-440, Edinburgh, UK, Aug.09-01-2005.

X. M. Rabaey, C. Savarese, J. and K. Langendoen, “Robust positioning algorithms for distributed ad-hoc wireless sensor networks,” in Proceedings of the 2002 USENIX Annual Technical Conference on General Track, pp. 317–327, USENIX Association, Berkeley, USA, 2002.

XI. N.Reijers, K.Langendoen “Distributed localization in wireless sensor networks: a quantitative comparison,” Computer Networks, vol. 43, no. 4, pp. 499–518, 2003.

XII. Schwabe, P,Bernstein, D.J. New AES software speed records. In: Chowdhury, D.R., Rijmen, V., Das, A. INDOCRYPT 2008. LNCS, vol. 5365, pp. 322–336. Springer, Heidelberg (2008)

XIII. Schwabe, P,Käsper, E.: Faster and timing-attack resistant AES-GCM. In: Clavier, C., Gaj, K. CHES 2009. LNCS, vol. 5747, pp. 1–17. Springer, Heidelberg (2009)