International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 3(A); March 2018; Page No. 10449-10452
DOI: http://dx.doi.org/10.24327/ijcar.2018.10452.1771

Research Article

TRUST BASED ENCRYPTION USING AES ALGORITHM OVER MALICIOUS ATTACKS IN WSN

Smitha P.S and Samuel John*

Velammal Engineering College

A R T I C L E I N F O

Article History:

Received 6th December, 2017
Received in revised form 21st January, 2018 Accepted 05th February, 2018
Published online 28th March, 2018

Key words:

TAES, FADER, Sensor, Nodes.

A B S T R A C T

Generally, in Static Wireless sensor networks a TRUST mechanism is implemented for reliable data packet transfer over the wireless network. The transfer takes place between sensors to sensor till it reaches its respective base station. Each sensor in the network are trusted nodes which is responsible for transmission. A sensor will have a limited amount of battery life. When the battery life reaches a certain limit it stops transmitting the packets to the neighboring nodes which makes it an untrustworthy node. In Existing system, the False Alarm Detection and Recovery (FADER) technique to detect these untrustworthy nodes. Apart from this there are various other malicious attacks are possible like flooding unrelated messages over the wireless network. In our proposed model using TAES we overcome these malicious attacks and provide a secure wireless sensing environment. We would be introducing the TAES to overcome the problems occurring in the existing model like reduced packet delivery ratio, reduced overall performance, more energy consumption, reduced trust value. We would include a threshold metric limit which would calculated with the help of interactions between the nodes and their trust values. These trust values are responsible for showing the trustworthiness of the nodes in the sensor network as by observing it we can conclude whether the node is malicious or not depending on its trust value with other nodes.

INTRODUCTION

Wireless Sensor Network (WSN) is a combination of Hardware and Software working together harmoniously over a fixed or closed area network. Sometimes it is also called as Wireless Sensor and Actuator Network (WSAN). A WSN consists of various components but few of them are *Sensors, Nodes, Base Station, and Graphical User Interface.* Certain areas are allotted were the sensors are placed per our requirements or to a certain procedure. Each sensor is responsible for collection the data from the physical world as it detects and

Responds to anything within its range, the sensor should be specified to collect data from which part of the physical world like light, heat, motion, moisture, pressure or any of the environmental phenomenon. The sensor is connected to a node via a wired medium. They are responsible for transmission the data collected from the sensor to the base station. The node can act in one-way communication where the node can only transmit the data to the base station which is for the purpose of monitoring only, two-way communication can act for both monitoring and control of the nodes. A WSN is made up of nodes where they can range from several hundreds to even thousands where each node is connected to several sensors.

Corresponding author:* **Samuel John
Velammal Engineering College

Security attacks in wsn

A WSN can be vulnerable to various forms of attack like spoofing, eaves dropping, unauthorized access and DOS attacks. Depending on the attacker location, way of attack or other possibilities the Security attacks on WSN can be classified into various ways. They can be majorly categorized into Outsider attack and Insider attack. The node whose security is compromised is known as malicious node.

- Selective Formatting,
- Spoofing,
- Outsider Attack,
- Sinkhole Attack,
- Sybil Attack,
- Physical Layer Attack,
- Network Layer Attack,
- Flooding Attack.

Trust Routing Protocols

A WSN consists of large amount of sensor nodes in the sensor network. As the sensor nodes within the network are required to communicate with each other the Routing protocols are used as a medium of communication between the sensor nodes and the base station. A Trust Routing Protocol is nothing but Trust mechanism implemented together implemented in this proposed work is Advanced Encryption Standard Algorithm or AES. It is implemented together with the basic trust evaluation

mechanism which leads to TAES. Advanced Encryption Standard (AES) is a more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays. It is also found that at least six times faster than triple DES. An algorithm was needed to replace DES because of its small key size. As the increase, in computing power DES was vulnerable to exhaustive key search attack. To overcome this drawback Triple DES was implemented but it was slow so AES was introduced.

AES has the Following Features

- It has Symmetric key symmetric block cipher.
- 128-bit data, 128/192/256-bit keys.
- It is faster and stronger than Triple-DES.
- It is software implementable both in C and Java.

Advanced Encryption Standard

AES is mostly based on 'substitution-permutation network'. It is an iterative cipher than Feistel cipher. It consists of a series of linked operations, some of which involve in replacing units by with the Routing protocol. The routing protocolspecific amounts or substitutions and other things involve in shuffling bits around or permutations.

The computation taking place in AES is performed on bytes instead of bits. So, AES would treat the 128bits of plaintext block as 16 bytes and these 16 bytes are arranged in a matrix form consisting of four columns and four rows. In AES, the number of rounds is variable and depends upon the length of the key, unlike DES. AES would use 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Here in this work we utilize 256-bit key.

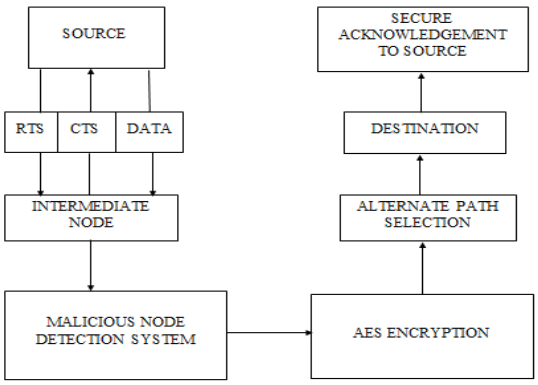


Fig 1 System Architecture

Encryption

A typical round of AES consists of four sub-processes. They are

- Substitution bytes or S-box
- Shift rows
- Mix columns
- Add round key

By using the fixed table in the S-box the 16 input bytes are substituted, which results in a matrix of four rows and four columns. Then each of the four rows of the matrix are shifted to left. The entries at the end are re-inserted on the right side of the row. It is carried as follows

- First row is not shifted.
- Second row is shifted one position to left.
- Third row is shifted two positions to left.
- Fourth row is shifted three positions to left.

The columns are transformed using a special mathematical function. The mathematical function takes the four bytes of one column as input and gives four completely new bytes as output. Which gives us a new matrix of 16 new bytes. The 16 bytes of the matrix is taken as 128-bits and XORed to 128 bits of round key.

Decryption

The decryption process is the inverse of the encryption process. It is as follows

- Add round key
- Mix columns
- Shift rows
- Substitution byte or S-box

Although they are similar sub-processes the algorithm for both encryption and decryption must be implemented separately.

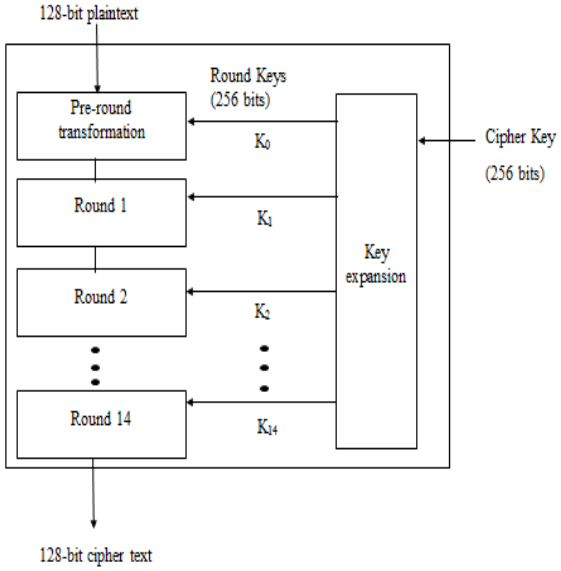


Fig 2 Structure of AES

Existing System

The Exisitng System explains that Insider packet drop attacks have become a serious threat to WSN. To distinguish a packet dropped by the inside attackers from network failure each node will use a trust mechanism to evaluate their neighbor nodes trustworthiness one problem associated with such trust aware routing algorithm is the False Alarm which occurs when a good nodes trust value goes down and being eliminated from the routing path this waste the networks resource and shortness the network lifetime as most trust mechanisms seek to aggressively identify attackers at the cost of increase in false alarm rate. [6] We propose a False Alarm Detection and Recovery technique to solve this problem instead of abandoning a node with low trust value from the network, we put it into an intermediate state between trust and untrusted know as suspicious node. We find alternate routing path for packet forwarding to guarantee networks packet delivery rate meanwhile we continue to send packet to the suspicious node and monitoring its trust value in order to determine whether

the node is untrusted or false alarm we have conducted extensive OPNET simulations and the results demonstrate that the proposed FADER approach can improve the performance of the trust aware routing protocol in terms of network lifetime, packet delivery rate and many other routing performance measures. FADER is able to recover at least 60% of the false alarms without recovering any of the real attackers this results in an average increase of about 40% in networks lifetime and can be as high as 83%.

Proposed System

This is based on Static WSN on a trust mechanism which is used for reliable data packet transfer between the nodes or from nodes to base station or vice versa over the network. This transfer takes place till the nodes are transferred from source to destination. A sensor will have a limited amount of battery life so the implemented routing protocols should provide necessary security and also efficient usage of the limited amount of resources. The existing work is possible for 2 nodes maximum within the network, if the number of nodes in the suspicious level increase the network is unable to maintain its efficiency and decreases the ratio of the packet drop, reduced trust value and few other problems are encountered. We tackle these problems by implementing a trust mechanism with a threshold value so if the trust value of the nodes is within the limits then they are within the networks if they are out of it then they are checked and reintroduced depending on the new values.

Topology Creation

Nodes are created to from a sensor network. The nodes send messages to communicate with each other and also to prove its presence in the network. The nodes are mainly of two types, they are Cluster head and Cluster member. Cluster member is a regular node with no new feature are implementations. Cluster head is a node within the sensor network where it acts as both the intermediate node and buffer between the nodes for communication between the nodes or send the data packets from the node to the Base Station. We have the power to decide the number of nodes which can be present within the WSN. We are also able to allot the amount of energy or the battery life to all the nodes within the sensor network.As the network used here is Static we are only able to decide the number of nodes in the network before the execution we are not able to include new nodes during the execution. We can only exclude a node from the network during the execution. Initially the source node would send an request message to the destination node or base station where the cluster head acts as buffer between the destination node or the base station. The destination node would reply with a message that it is clear, then a link is established between the source and destination. Then the destination node or the base station starts receiving the data packets and it would send back an acknowledgement to the source, this process would be repeated till the transmission would be completed.A cluster head is generally assigned from the base station as they monitor the logs of the nodes. The node with the high battery value would be assigned this responsibility as it has the sufficient resources to do this king of activity.

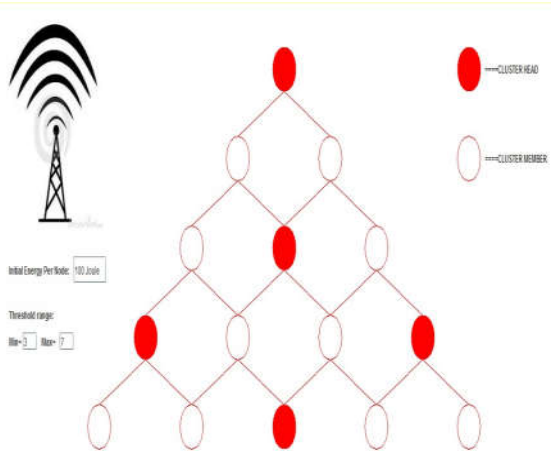


Fig 3 Network Structure

Aes implementation

AES is a block cipher providing a symmetric-key algorithm. Encryption plays a major role in data transfer between the nodes or from node to base station it prevents the third party unauthorized access to it. An encryption model with less resource consuming and has provide more message integrity AES fits this profile as it is one of the best encryption method of now as it is faster than DES and with much more sophisticated uses. When an attacker would try to hijack a node a try to decrypt the data within the node it is of high difficulty as AES uses a key mechanism which would only be at the source and destination end and the encrypted message can only be decrypt with this key.AES provides us with different cipher keys as of like 128-bit, 192-bit and 256-bit. Here the cipher key used is 256-bit as it provides highest possible encryption. In AES, each time the generated cipher text is unique and it is humanely impossible to identify any sequence or series of any kind from the cipher text.It is also less susceptible to cryptanalysis than 3DES. When the malicious node is detected in the system the transmitted data would undergo encryption using AES and the key for it would only be with the source and destination end and it is not easy to decrypt the message without the help of the key. An alternate path would be selected when a malicious node is detected within the system. The router is responsible for finding the alternate path between the source and destination. The further message passed would also be encrypted after the detection of the malicious node. The AES provides a better and energy conservative encryption along with the trust mechanism. These two implemented together would provide secure, efficient mechanism to implement in the nodes of WSN.

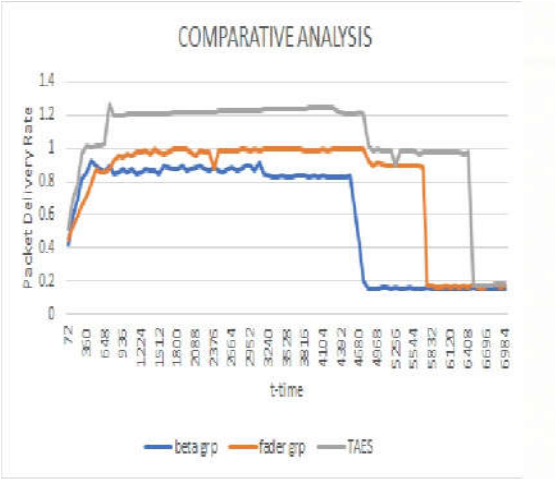
Detection of Malicious nodes

In the Static sensor network a certain number of nodes are placed covering a specified area. The nodes has a specified amount of battery life. The trust value of a node defines whether it is trustworthy or not and neighboring nodes prefer it to transfer the data through it. If the trust value of the node is 1 then it is trustworthy, if the trust value of the node is 0 then it is not trustworthy. Initially all the nodes within the network are allotted a trust value of 1. The trust value would be calculated depending upon the behavior of the node.The nodes behavior would by the administrator through the base station. The trust value would be calculated by the ‘sum of trust value of the node in each session divided by the total number of session

multiplied by 100'. If the resulting value is 100 then the node is trustworthy if it isn't then the node is not trustworthy.

CONCLUSION

In this work, a method for tracking and detection of malicious nodes has been proposed. As the use of wireless sensor networks (WSN) has increased, the security in WSN has also become more important. It is shown that effective way of utilising the existing methods and deriving a new method also provides us with better results. We discussed different types of attacks like misbehaviour and malicious nodes. FADER is mainly dependent on trust mechanism but our proposed work includes both the trust mechanism and also a data encryption like AES which provides high integrity.



Future work

In future, efforts can be taken to extend or optimize the efficiency of the battery life in the sensor node. Advanced algorithms can be used to evaluate and identify the vulnerabilities in WSN to ensure that proper measure can be taken.

References

1. Azzedine Boukerche *et. al*. "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", vol.3, pg.5 in 2005.
2. Surinder Singh *et. al*. "Sensors Augmentation Influence over Trust and Reputation Models Realization for Dense Wireless Sensor Networks", vol.15, Issue: 11, Pages: 6248 - 6254 in 2015.
3. Xue Wang *et. al*. "Trust Evaluation Sensing for Wireless Sensor Networks", vol.60, Issue: 6, Pages: 2088 - 2095 in 2011.
4. Fenye Bao *et. al*. "Trust-Based Intrusion Detection in Wireless Sensor Networks", Pages: 1 - 6 in 2011.
5. Jun Peng *et. al*. "Communication Scheme in Trusted Sensor Network", vol: 2, Pages: 10 – 13 in 2010.
6. Youngho cho *et. al*. "Enhancing Trust-aware Routing by False Alarm DEtection and Recovery", Pages: 52 - 59 in 2014.

How to cite this article:

Smitha P.S and Samuel John (2018) 'Trust Based Encryption Using Aes Algorithm Over Malicious Attacks in WSN', *International Journal of Current Advanced Research,* 07(3), pp. 10449-10452.
DOI: http://dx.doi.org/10.24327/ijcar.2018.10452.1771

****