ISSN 2319 - 6629

Volume 6, No.3, April – May 2017

International Journal of Wireless Communications and Networking Technologies

Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt02632017.pdf

Securing WSN From False Injection Data Attack Using RSA Based Security System

Vishwaraj[1] **and Bharath.S**[2]

[1,] Department of Electronics and Communication Engineering, UBDT College of Engineering, Davangere, Karnataka, India

[1] vishwarajbm@gmail.com

[2]Department of Electronics and Communication Engineering, UBDT College of Engineering, Davangere, Karnataka, India

[2] bharath.s828@gmail.com

ABSTRACT

Wireless sensor networks (WSNs) consists of enormous set of sensor nodes along with co-operative network, restricted power supply and constrained computational capability[3]. In wireless sensor networks packet forwarding is generally carry out through multi-hop data transmission due to restricted communication range. Since sensor networks deployed in wide range therefore security will be the main obsession to be considered [4]. Usually the deployment of WSNs able at the unaccompanied or adverse atmosphere. Hence, the networks are attacked by adversary who agency to accident the activity of the arrangement by compromising the sensor nodes and animate artificial advice or bogus information into the networks. Hence it is essential to protect sensor network from the attack of bogus information injection [1]

Key Words: Network protocols, wireless network, mobile network, wireless sensor networks (WSN), RSA algorithm

1. INTRODUCTION

1.1 Problem Formulation

The existing detection methods can sense the pack injection attack that from compromised sensor nodes in a WSN using various routing protocols. MAC algorithm acclimated in the existing schemes accommodate alone affidavit to the system but MAC algorithm suffers from cryptographic weakness. In this work, we propose RSA algorithm to accomplish the system more secured and to overcome from cryptographic weakness.

1.2 Objective

This work determines the implementation of RSA based security scheme along with on-demand routing preventing the attack of false data injection in WSNs in accordance with NS-2 simulation. Algorithm acclimated in the modified scheme provides greater protection to the system than MAC algorithm in the BECAN scheme. MAC algorithm provides alone an affidavit or authentication to the system but RSA algorithm makes the system more protected by public key cryptographic technique.

1.3 Methodology

Methodology for securing wireless sensor networks using Rivest Shamir Adleman (RSA) algorithm is divided into four main sections, they are Network model, Security model, Routing model and information forwarding. In the network model a set of sensor nodes are deployed at certain area or region of interest and each sensor nodes are equipped with Omni-directional antenna. After that security keys are generated for each and every sensor nodes in security model using RSA algorithm. In the routing implementation we are using reactive routing protocol called on-demand routing protocol [2]. Finally in the information forwarding, information is forward from source node to destination node through routing paths.

2. PROPOSED SYSTEM

A security scheme is outlined utilizing RSA algorithm to evade cryptographic shortcoming. RSA algorithm is utilized as a part of this change and it is utilized for producing and building up pair wise key routing protocol worn is dynamic source routing. A large sort of nodes broadcast throughout an acreage accumulate together, authorize a routing topology, also address abstracts aback to an accumulating point. The proposed system enclose RSA algorithm includes block diagram of modified security scheme have four major building block, namely network model, security model, routing topology and information forwarding.

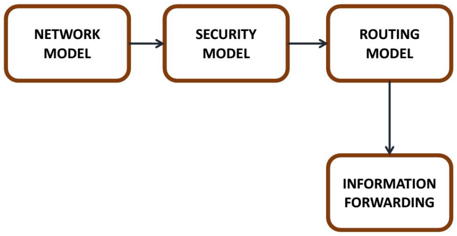


Figure 1: Proposed Model

2.1 Network Model

Network model defines how the arrangement is formed. In this cardboard accept a wireless sensor arrangement accepting small set of sensor nodes. The system is partitioned into addressable locales. Every locale contains an arrangement of sensor nodes. A sample of such an association can be given utilizing a base station, or a sink, that serves as a focal point of a polar coordinate system. The separation between a sensor and the sink is resolved taking into account the base-station sign level, as abstinent by the sensor node.

In this network model large amount of sensor nodes are about positioned at a certain region of interest (CIR) along with the breadth ‘S’ in WSN. Arrangement model consists of sink which is an accurate and able abstracts accumulating device. Each sensor node is outfitted with Omni-directional reception apparatuses. The communication between the nodes is bidirectional, which means two sensor nodes inside of their remote transmission range may speak with one another. Since some sensor nodes resides very close to sink and hence they have direct contact with sink node during information forwarding.

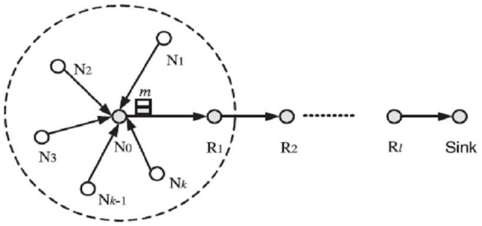


Figure 2: Network Model

2.2 Common Types of Network Attacks

The most common type of attacks are Eavesdropping, Identity Spoofing, Selective Forwarding or Grey Hole, Sink Hole attack, Worm Hole attack, DoS, Application layer attack, Compromised key attack

In this proposed scheme to protect sensor network from various types of attack, cryptography is used along with the RSA algorithm in the security model. RSA is an asymmetric type cryptography which includes two types of keys specifically public key and the private key. The network security based on RSA algorithm must provide following services, they are integrity, data confidentiality, authentication, non-repudiation and entity authentication these are illustrated as shown in figure 3.

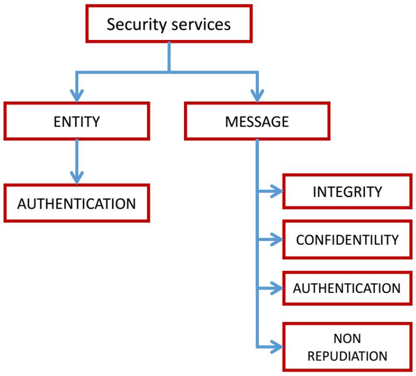


Figure 3 Different types of security services

3 SYSTEM IMPLEMENTATION

Wireless sensor networks comprises of nodes that move uninhibitedly or freely and commune with others through wireless links. In this proposed work the nodes that are randomly deployed and connectivity also be done by randomly. One approach to assistance efficient commune between nodes in less intense network is to build wireless backbone architecture by discovering neighbours from base station.

3.1 Model Definition

Model definition gives an unmistakable perspective of the proposed work since this algorithm tries to increment collaboration between nodes and increases the security level in the network. It can be estimated that the reason for loss of packets in the network due to non-co-operative activities of nodes in wireless communication channel. In sensor network, since nodes are resource controlled, a few nodes are liable to accumulate power to stay in the network.

3.2 High Level Design

Design is a standout among the most imperative periods of software development. Since the design is an innovative process in which the system framework is set up that will fulfil the functional and non-functional requisites [5]. Large systems are frequently decayed into subsystems that give some related sort of services. The productivity of the design process is a portrayal of the software architecture. The simulation of security aspects of WSN can be categorized as node deployment, routing management, implementation of RSA algorithm, false data detection, energy efficiency and information forwarding.

3.3 System Architecture

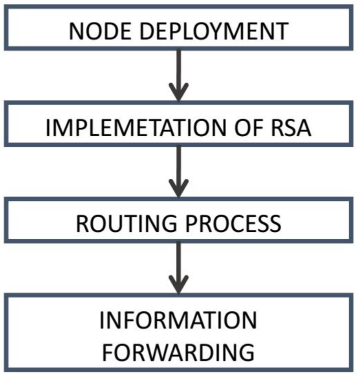


Figure 4. System Architecture

3.4 Node Deployment

In WSNs deployment of nodes which is an application dependent and influences the execution of the routing protocol. The nodes deployment can be catogorized either deterministic or randomized. In this proposed work the node are deployed in random nature. For the random deployment of nodes, every nodes are randomly scattered making a framework in an ad-hoc mode. On the off chance that the allocation of resultant nodes is not identical, optimal clustering gets to be important to allow network and empower energy proficient netwok operation. There is another type of communication i.e. inter-sensor communication is typically inside of short transmission range because of energy and data transfer capacity restrictions.[6] In this manner, it is probably that a route will comprise of severel multiple wireless hops.

Since the sensor nodes sense the information from environment. Every sensor node made some calculation in view of sensed information. Each sensor nodebe in contact with other sensor nodes and base station to make an outcome based on processed information.The architecture WSN nodes is shown in the figure 5.

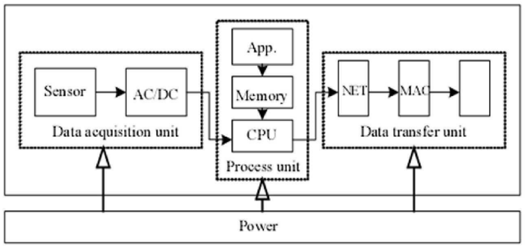


Figure 5 Sensor Node Architecture

In this proposed work,consider there is an wireless sensor network model comprising 40 sensor nodes and these are deployed to random location in certain region of interest with area S. This network model consist of sink node which trustable and powerful, and it has capability of receivig data from the each and every nodes within a network. All the nodes are equipped by means of omni directional antennas and the sensor nodes which are nearer to the sink node have direct commune with sink node that means exchange the data or information directly. In this model communication is bidirectional, since two sensor nodes interact with each other within an communication range (R).

3.5 RSA Algorithm

Three cryptographers Rivest, Shamir and Adleman who are the inventers of the RSA security algorithm. The RSA algorithm was publicly described in 1978. Since RSA is an assymetric type security protocol as it uses two distinct keys for its encryption and decryption reason. It is also known as public key cryptography. Since RSA is the first algorithm referred to be appropriate for marking/signing and in addition encryption, and was one of the first powerful as well as best advances in public key cryptography [8]. RSA is broadly utilized as a part of electronic.

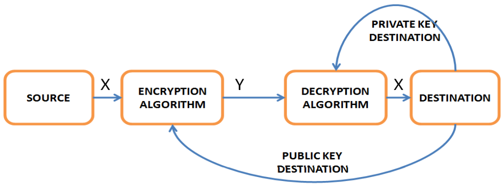


Figure 6: Security scheme in RSA

RSA Security Protocol

Since RSA algorithm comprise of three processing steps , namely generation of keys, encryption process and decryption process.

(a) Generation of Keys:

The RSA algorithm includes two types of keys public key and a private key. Since the public key is broadcast to everyone hence it is known to everyone and is utilized for encoding or encryption of messages. Generation of keys for RSA algorithm is illustraded in following steps:

1) Select two numbers ‘r’ and ‘s’ randomly which are prime number, and there is an condition that r != s. For security issue, the numbers r and sare to be picked uniformly at random and should be of comparative bit-length.

2) In the next step computing integer ‘n’ by n = rs. Here integer ‘n’ is is used as modulus for both the security keys.

3) Calculate phi, $\varphi(n)= (r-1)(s-1)$, where $\varphi(n)$ is the totient of ‘n’.

4) Pick an integer‘E’ such that $1 < E< \varphi(rs)$, and e and $\varphi(rs)$ are not having any devisor other than 1 i.e., E and $\varphi(rs)$ are coprime ($\gcd(E, \varphi) = 1$) E is designated as exponent of public key E having a short bit-length and little Hamming weight brings about more effective encryption.

5)Now find out D (by using mod arithmatic) which fulfills the equivalencerelation

$DE=1 \pmod{\varphi(rs)}$ or $D= E^{-1} \bmod \varphi$

Here integer D is designated as private key exponent.

(b) Encoding Process:

In the encryption or encoding process, receiving user broadcast his public key (n, E) to the sending user and retains the private key secrete. Then sender wants to send the information or message ‘M’ to the receiver. By using padding scheme the sender transforms ‘M’ to integer $0< M <n$. After that sender convert the plain text (original message) M into cipher text (encoded message) U is illustrated as

$U=M^{E} \bmod n$

This encrypted message is send to the receiver by sender using receiver public key.

(c) Decoding Process:

At the receiver side encrypted message U is decrypted to original message format M is done only by using private key of the receiver (D, n). The following equation illustrate the decryption process

$M=U^{D} \bmod n$

The discovery of the route is initiated when the source node doesn’t have any routing knwoledge to the destination. The route discovery procedure is starts with broadcasting RREQ message through the network, it is shown in the figure below. Upon receiving RREP message by source then route is established. Suppose if multiple packets along with different routes are received hence by means of greater sequence number of these RREP messages the routing information is updated.[7]

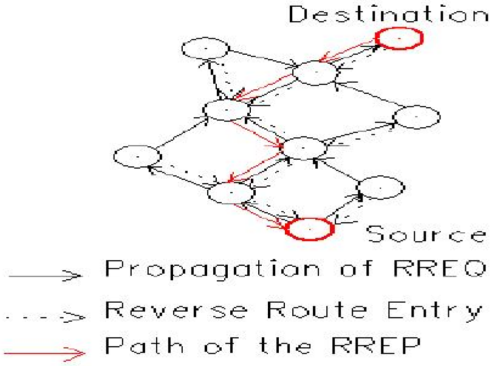
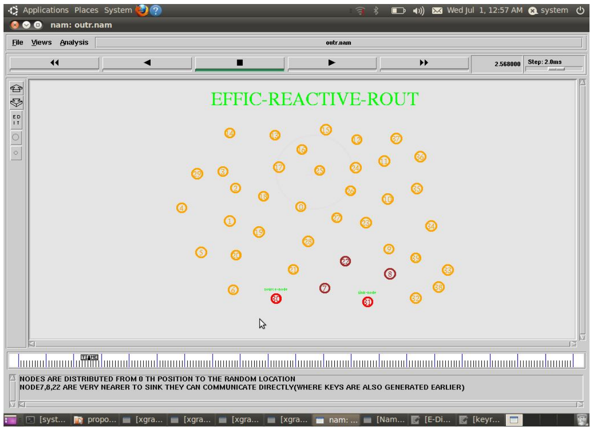


Figure 7 Route Discovery in AODV

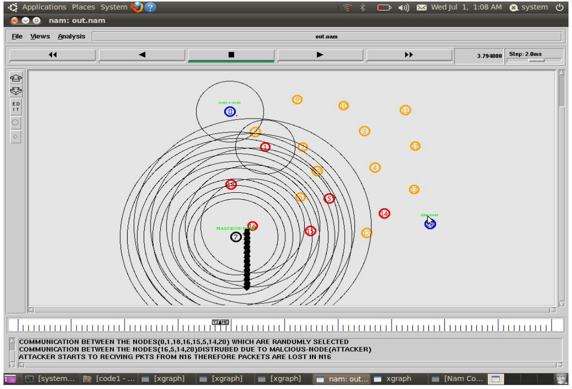
4. RESULTS

The proposed work shows the implementation of RSA algorithm in the security model implementation is carried out in network simulator 2 using tool command language. The result includes snapshots and graphs of simulation of proposed and existing system in terms of network animator, trace file, throughput, energy efficiency, control overhead and packet delivery ratio.



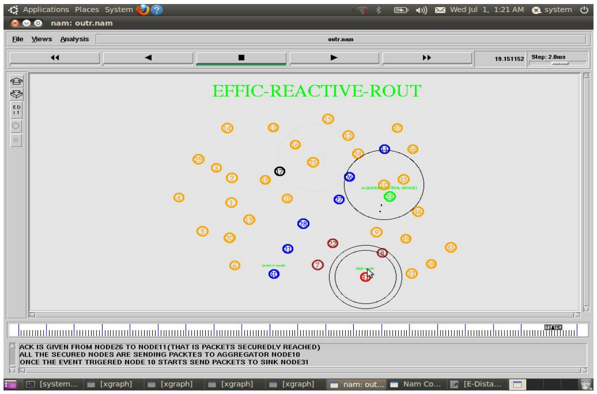
```
NODES ARE DISTRIBUTED FROM 0 TH POSITION TO THE RANDOM LOCATION
NODE7,8,22 ARE VERY NEARER TO SINK THEY CAN COMMUNICATE DIRECTLY(WHERE KEYS ARE ALSO GENERATED EARLIER)
```

Figure 8: Nodes deployment in network



```
COMMUNICATION BETWEEN THE NODES(0,1,18,16,15,5,14,20) WHICH ARE RANDUMLY SELECTED
COMMUNICATION BETWEEN THE NODES(16,5,14,20)DISTRUBED DUE TO MALCIOUS-NODE(ATTACKER)
ATTACKER STARTS TO RECIVING PKTS FROM N16 THEREFORE PACKETS ARE LOST IN N16
```

Figure 9: Packet loss in existing system due to attacker (Animator file)



```
ACK IS GIVEN FROM NODE26 TO NODE11(THAT IS PACKETS SECUREDLY REACHED)
ALL THE SECURED NODES ARE SENDING PACKTES TO AGGREGATOR NODE10
ONCE THE EVENT TRIGERED NODE 10 STARTS SEND PACKETS TO SINK NODE31
```

Figure 10: Successful packet transmission in RSA based WSN

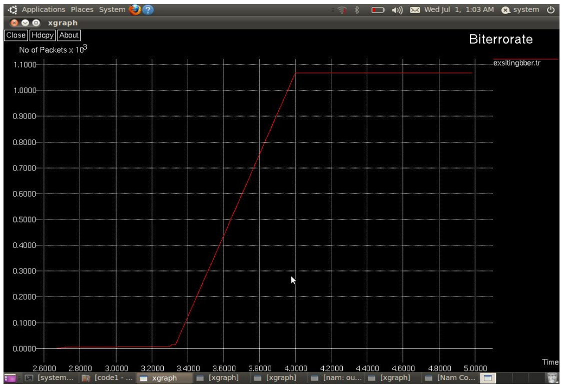


Figure 11: Bit error rate of existing system

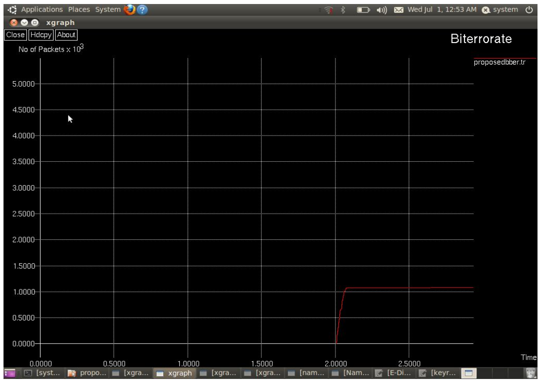


Figure 12: Bit error rate of RSA based WSN

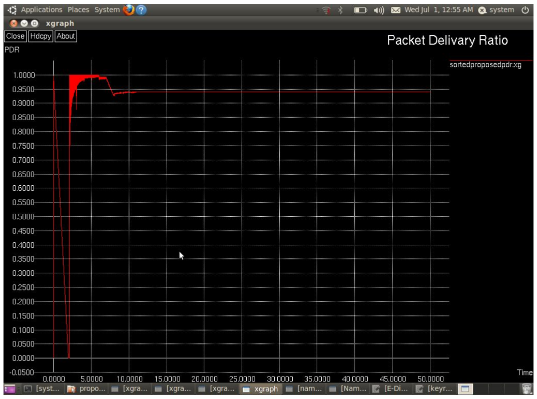


Figure 13: Packet delivery ratio of RSA based WSN

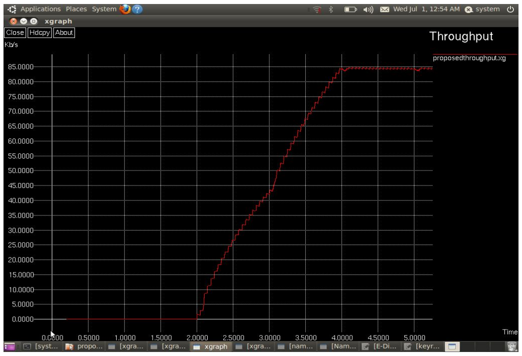


Figure 14: Throughput of RSA based WSN

5. CONCLUSION

This work conclude that the performance of security proposal based on RSA algorithm with AODV (Ad-hoc On-demand Distance Vector) for preventing bogus information or false data injection attack in wireless sensor network using Network Simulator-2 simulation tool. The modified scheme adapting RSA algorithm provides greater security to the system when it is compared with BECAN (Bandwidth efficient Co-operative authentication) scheme having MAC algorithm. The work also shows that, the output metrics such as energy, packet delivery ratio and throughput have higher values in performance of RSA based security scheme.

REFERENCES

[1] F.Ye, H. Luo, S.Lu, and Zhang, **“Statistical En-Route Detection and Filtering of Injection False Data in Sensor Networks.”** Proc IEEE INFOCOM’ 04 Mar. 2004. 43-856, 2010

[2] S. Zhu, S. Setia, S. Jajiodia and P.Ning **“An Interleaved Hop-by-Hop Authentication scheme for Filtering of Injection False Data in sensor Networks”** Proc, IEEE symp. Security and Privacy, 2004

[3]H.Y Yang, F.Ye, Y Yuan, S.Lu and W. Arbaugh, **“Toward Resilient Security in Wireless Sensor Networks,”** Proc. Sixth ACM Int’l symp Mobile As Hoc Networking and Computing (Mobi Hoc ‘05), pp 34-45, 2005

[4]K. Ren, W. Lou, and Y. Zhang**,”LEDS: Providing Location-Aware End to-End data security in wireless Sensor Networks”**, Proc IEEE INFOCOM ‘06Apr. 2006.

[5]Y. Zhang, W. Liu, W. Lou and Y. Fang. **“Location-based compromise-Tolerant Security Mechanism for Wireless Sensor Networks”** IEEE Selected areas in Comm, Vol 24, no 2, pp 247-260, Feb. 2006.S

[6]Rongxing Lu, Student Member, IEEE, Xiaodong Lin, Member**,”BECANA bandwidth-efficient,cooperative Authentication Scheme for Filtering scheme for Filtering Injected False Data in Wireless Sensor Networks”** IEEE transactions on parallel and distributed systems, vol. 23, no. 1, January 2012.

[7] Ankit Bhardwaj, Divya and Sanjeev Sofat, **An Efficient Energy Conserving Scheme for IEEE 802.11 ADHOC Networks‖,** IEEE 1-4244-1005-3/07, 2007.

[8] R.L. Rivest, A. Shamir, L.M. Adleman, **“A method for obtaining digital signatures and public keycryptosystems”**, Communications of the ACM 21(2) (1978) 120–126.