Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Wormhole Attack Countermeasures for Spontaneous Wireless Network Using Paillier Cryptography

Snehal Rane
Department of Computer Engineering
Sinhagad Institute of Technology,
Lonavala, Maharashtra, India

Dr. Babar S. D.
Head of Department of Computer Engineering
Sinhagad Institute of Technology,
Lonavala, Maharashtra, India

Abstract: Overdue to attributes of open medium, absence of framework, dynamic network topology, cooperative algorithms, lack of centralized monitoring and resource constraints, ad hoc networks are unprotected to many kinds of attacks, among which wormhole attack is chosen as the topic of discussion. This attack, when launched during route finding phase can penetrate incorrect route/topology data into the network thereby, beat the intention of routing algorithms. Wormhole Attacks in ad-hoc networks can be immensely disturbing in some conditions specifically when they lead to Rushing Attacks. Our presented solution in a wormhole attack countermeasures for Spontaneous wireless network using paillier cryptography aims to combat these attacks by separating the network up into clusters/groups depends on contiguity of nodes and other factors. All messages now (Route Request in the case of AODV routing) will be sent through a secured node which is also made the cluster-head. We present adding a protection for data aspect comprising of security technique paillier cryptography when it is passes through each cluster-head node. Also we proposed algorithm for Maximum Energy Base routing Under MANET .By using this Algorithm we can change path for sending data.

Keywords: AODV, TAODV, MANET

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) contains mobile nodes capable of forming networks on the fly, without a common point of communication or central infrastructure. Ad hoc networks have solved real world issues of heavy infrastructure needs, stillness of nodes and dependency of nodes on one central node to form a network. Ad hoc networks have taken many forms like low cost infrastructure depends on Sensor Network (SNS) recording environmental changes at a location or capturing the battlefield scenario. They have also been successfully extended to upcoming field of Vehicular Ad hoc Networks (VANETs) to ensure road safety.

Due to their wireless nature, ad hoc networks are prone to a numerous attacks such as Sybil attack, Black Hole attack, Rushing attack, and Wormhole attack etc., launched by malignant nodes. Since nodes in an ad hoc network also function as routers that finds and handle routes to other nodes in the network, if routing is misdirected, the whole network will be paralyzed. Thus, routing security plays an important role in the security of the entire network. In this paper we focused on avoidance of the Wormhole attack launched by malignant nodes[1].

Wormhole Attacks in ad-hoc networks can be immensely disturbed in some condition specifically when they lead to Rushing Attacks. Our presented solution in “wormhole attack countermeasures for spontaneous Wireless network using paillier cryptography” aims to defend this attack by using paillier cryptography. It is asymmetric algorithm used in public key cryptography. In this public key and private keys are generated and stored on nodes. For encryption we are using public key (n, g) and for decryption using private key (λ, μ).In this cryptographic technique source node encrypt data by using public key and destination decrypt it by using private key. So if data came from malicious node it can’t decrypt. In this way we can find out wormhole attack.

Rest of the Paper Will Organize as follows: In Section II we discuss about the related work on the prevention and detection of wormhole attack .In Section III ,we describe our encryption and wormhole prevention algorithm in detail. While section IV present simulation results and conclude the paper in section V.

II. RELATED WORK

Recently, we have seen the evolution of second- and third-generation wireless systems that incorporate the features provided by broadband. In addition to supporting mobility, broadband also aims to support multimedia traffic, with quality of service (Quos) assurance. We have also seen the presence of different air interface technologies, and the need for interoperability has increasingly been recognized by the research community. As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems [1, 2].

Packet Leash is one of the first techniques of wormhole attack prevention. In Geographical Leashes, a node before sending a packet adds its position and a timestamp to it. When other node receives the packet, it checks the time stamp of sending node and current time and thus calculates distance between them. If this exceeds threshold distance, the packet is discarded. Whereas, in Temporal Leashes (where nodes require tight time synchronization), a node appends time stamp while sending the packet which is compared by present time when received by other node and expiration time is calculated which if exceeded, results in discarding of the packet. This method requires additional hardware to fulfil GPS requirements and/or accurate time synchronization [3].

Mobile Ad-hoc Network (MANET) is a self-configuring without infrastructure network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. MANET does not require any fixed infrastructure and it is capable of self-configuring, these unique characteristics made MANET ideal to be deployed in a remote or mission critical area like military use or remote exploration. However, the open medium and wide distribution of nodes in MANET leave it vulnerable to various means of attacks. This paper proposes a TAODV for improving security in adhoc routing protocol [4].

We propose a novel algorithm for detecting wormhole attacks in wireless multi-hop networks. The algorithm uses only connectivity information to look for forbidden substructures in the connectivity graph. The proposed approach is completely localized and, unlike many techniques proposed in literature, does not use any special hardware artifact or location information, making the technique universally applicable [5].

Wireless Sensor Network provides various applications like military, healthcare etc. These types of applications required a certain level of security. WSN is exposed by various types of attacks; wormhole is one of severe attack on WSN. In wormhole attack, an attacker receives packet from one location pass them through the tunnel and release to them another location. We propose an algorithm which defends wormhole attack in WSN called public key encryption and 2Ack based approach [6].

III. IMPLEMENTATION DETAILS

III.1 Paillier Cryptography

The Paillier Cryptosystem is well known Homomorphic encryption invented by and named after France researcher Pascal Paillier in 1999 is a probabilistic asymmetric algorithm for public key cryptography.

The public cryptography use asymmetric key algorithms, where the encryption and decryption key are different. Every user in the process has a pair of cryptographic keys:

a public key and a private key. The private key is kept secret (unknown to other users)and public key may be widely distributed. Messages are encrypted with the public key and be decrypted with the corresponding private key. The scheme Paillier Cryptosystem works as follows:

1. Key generation

- Select two large prime numbers a and b arbitrary and independent of each other such that gcd(n, Φ (n)) = 1, where Φ(n) is Euler Function and n=ab.
- Calculate RSA modulus n = ab and Carmichael's function is given by λ = lcm(a-1, b-1).
- Select g called generator where

$g \in Z_{n_2}^*$ Select α and βrandomly from a set
Z_n^* then calculate $g = (\alpha n + 1)\beta^n modn^2$.

- Compute the following modular multiplicative inverse μ= (L (g $^{\lambda}$mod n2)-1mod n. Where the function L is defined as L(u) = (u - 1)/n.

The public (encryption) key is (n and g).
The private (decryption) key is (λ and μ).

2. Encryption

(a) Let mess be a message to be encrypted where mess∈ Zn.

(b) Select random r where $r \in Z * n2$.

(c) The cipher text can be calculated as:
cipher =$g^{mess} \cdot r^n \cdot modn^2$.

3. Decryption

(a) Cipher text c ∈ $Z * n2$.
(b) Original message: mess = L (cipher λ mod n2)· μ mod n.

III.2 Cluster head election procedure

There are some criteria for selection of cluster head as follows. The procedure consists of eight steps as described below:

1. Find the neighbors of each node v (i.e.., nodes within its transmission range) which
Defines its degree, d_v, as

$$d_v = |N_v| = \sum v' \varepsilon V, v' = V\{dist(v', v)\}¡ tx_{range}$$

2. Compute the degree-difference,
$\Delta v = |dv-\delta|$, for every node v.
3. For every node, compute the sum of the distances, D_v, with all its neighbors,
4. Compute the running average of the speed for every node till current time T . This Gives a measure of mobility and is denoted by M_v,
5. Compute the cumulative time, P_v, during which a node v acts as a clusterhead[5].
$P_v$implies how much battery power has been consumed which is assumed more for a cluster head than an ordinary node.
6. Calculate the combined weight Wv for each node v,

$$W_v = w1\Delta v + w2D_v + w3M_v + w4P_v,$$

7. Choose that node with the smallest WV as the cluster head. All the neighbors of the chosen cluster head are no longer allowed to participate in the election procedure.
8. Repeat steps 2-7 for the remaining nodes not yet selected as a cluster head or assigned to a cluster.

III.3 Algorithm for Maximum Energy Base routing Under MANET

After detection of wormhole attack, need to select the best path for data transmission. so we proposed algorithm for best path selection as follows :

```
1. Create mobile node = N;
2. Set routing protocol = AODV; // (for Routing Protocol)
3. Set of N = Vs ,Vd, Vi, Vj, Vk, Vl, .... Vn //(Number of mobile nodeas)
4. Set of Intermediate vertex or node's Vi, Vj, Vk, Vl, ....
Vn$\varepsilon$N,
5. Set sender = Vs;
                    Vs $\varepsilon$ N
6. Set Destination = Vd;
                    Vd$\varepsilon$ N
7. Set initial energy of each node E = es, ed, ei, ej, ek, el,.... en
8. Compute Route (Vs, Vd, E, rr)
9. If (path exist from Vs to Vi, Vi != Vd,) Increment pointer Vi as Vj and Vs as Vi Broadcast route packet to next hop
10. If (Vj == Vs)
{
Create rtable in Vs Node
Create energy table Vs-Vi-Vd
}
11. If (path[n] > 1)
12. {
if (path Vsijd from S to D path Vskld from S to D)
}
for Each path except malicious path maintain Energy table
Create rtable Vs via path Vij to Vd
Create energy table es via path eij to ed
Create rtable Vs via path Vkl to Vd
Create energy table es via path ekl to ed
} }
13. Find Max-eng (ej, ek)
14. {
if (ej max-eng)
select the path which has maximum energy Select route Vs via path Vij to Vd
}
15. End
```

Mathematical Model

The system S is represented as: S={ I, C, K, L, M }
A. Input is number of vertices and set of characters to the system.
Let I is the set of input
I1= $\{i11, i12, i13, \ldots . i1n\}$
I2= $\{i21, i22, i23, \ldots . i2n\}$
Where
i11,i12,....i1n are the set of vertices and i21,i22,i23,...i2n are the set of characters.
B. Cluster Generation
Let C is the set of cluster.
C1=$\{c1, c2, c3, \ldots cn\}$
Where
c1,c2 c3,...cn are the set of cluster.

C. Path Finding

Let K is the set of source node, Cluster head, Gateways, and destination node.

K=$\{sn, ch, g, dn\}$

Where,

sn is Source node, dn is Destination node, ch is Cluster Head and g is Gateways.

D. Encryption of string

Let L is the Encryption process.

L=$\{e\}$

Where, e is the encryption string

E. Decryption of string

Let M is the Decryption process.

M=$\{d\}$

Where, d is the decryption string

F. Send string to destination node

Let O is the string which is transmitted towards destination.

O=$\{o\}$

Where,

o is the string message which is transmitted to the Destination node.

IV. RESULTS

This section evaluates the performance of the proposed scheme with and without the presence of wormhole attack. Compare its efficiency on the basis of time and energy.

The following graph shows that wormhole channel required maximum time comparedto changed path channel.

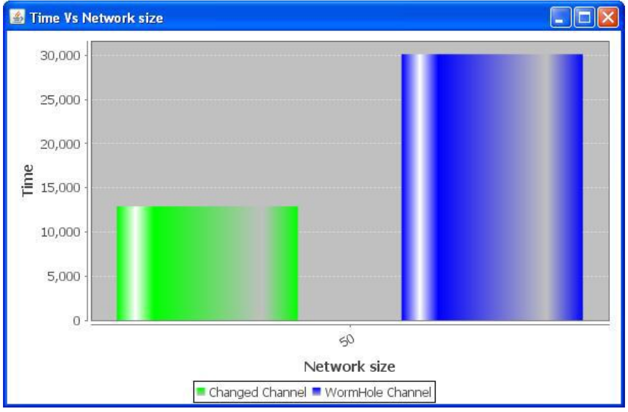

Fig.1: Graph of comparison for wormhole channel and changed path channel According to the time required

The following graph shows that wormhole channel required maximum energy compared to changed path channel

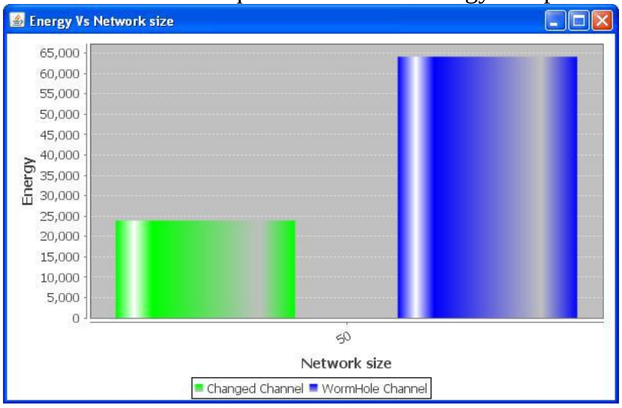

Fig2: Graph of comparison for wormhole channel and changed path channel according to the energy required

V. CONCLUSION

We develop a novel method for avoidance against worm hole attacks. Compared to conventional routing protocols, our presented method enhances information protection via robustness against the wormhole attack. It integrates principles of clustering and digital signatures during searching and establishment of routes in reactive routing protocols. Simulation outputs prove the effectiveness of the presented method in existence of wormhole nodes. The first phase of the project involved analyzing about MANETs and protection threats prevalent. After reading about types of security threats, we analyzed more about Wormhole attacks and the methods of paillier cryptography devised to prevent them. Based on the research and previous work done, the protective clustering approach as advised by us seems promising in combating wormhole attacks.

REFERNCES

[1] Chai K Toh"Ad Hoc Moblie Wireless Networks: Protocols and Systems", December 2001.

[2] Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE, "Wormhole Attacks in Wireless Networks", FEBRUARY 2006

[3] Yih-Chun Hu, Adrian Perrig, David B. Johnson, Carnegie Mellon University, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks.

[4] *R. Sathya, Dr.P. Latha,* An Effective Security Approach for MANET using Detection Algorithm, 2012

[5] Ritesh Maheshwari, Jie Gao and Samir R Das Department of Computer Science, Stony Brook University Stony Brook, NY 11794-4400, USA, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", 2002.

[6] Pravin Khandare, Prof. N. P. Kulkarni, Department of Information Technology, SKN College of Engineering Pune-41, India, Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack, 2013.