# Thwarting Sybil Attack using ElGamal Algorithm

Shefali Khatri
Department of CSE
Uttaranchal University
Dehradun

Punit Sharma
Department of CSE
Uttaranchal University
Dehradun

Arvind Negi
Department of CSE
Uttaranchal University
Dehradun

Himanshu Gupta
Department of CSE
Uttaranchal University
Dehradun

## ABSTRACT

MANET is an independent and infrastructureless network comprising of self configurable mobile nodes connected via wireless links. MANET is susceptible to various attacks because of some loopholes present in MANET like dynamic topology, zero central administration, limited physical security etc. MANET is prone to numerous malicious attacks one such attack among them is SYBIL ATTACK. In Sybil attack multiple identities are presented by a single physical node. This attack has serious impact on network functionality. In this paper principle focus is on preventing Sybil attacks using ElGamal algorithm. The concept of ElGamal algorithm has been used in this paper so as to deal with Sybil attacks.

## General terms

Sybil, ElGamal, Legitimate

## Keywords

MANET, Random sub key, swapping

## 1. INTRODUCTION

In contradiction to infrastructured wireless networks, where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET, is an autonomous and decentralized wireless system that does not rely on a preset infrastructure for its operations. The network is composed of mobile nodes that communicate with each other via wireless links. Nodes that lie within the proximity of each other are capable of communicating with each other directly whereas nodes that are not within each other's radio range, communication between them is conducted by granting assistance from intermediate nodes that acts as routers that relay packets generated by other nodes to their destination. MANET is gaining popularity at an alarming rate as it provides wireless connectivity regardless of geographic position. MANET is defined as a network that consists of autonomous nodes that has the potential to organize them into different network topology. MANET is a dynamic network comprising wireless mobile nodes that communicate over relatively bandwidth constrained wireless links.

Nodes in MANETs can join and leave the network dynamically [1]. MANET is more susceptible to security attacks than wired networks because of some notable vulnerabilities present in MANET like zero central administration, dynamic topology, lack of clear line of defense, compromised node posing threat inside the network, battery constraints etc. because of these features MANET is highly susceptible to different attacks. There are numerous attacks that target different layers in MANET. Sybil attack is one of the most devastating attacks in MANET that target the network layer. Sybil attack intents to disrupt normal functioning of the network by spoofing the identity of the legitimate node. Here the intruder forges multiple identities for malicious intent. Sybil attack aims at hampering trustworthy and reliable communication in the network.

## 2. LITERATURE SURVEY

Nidhi et al. [2] in her paper combined the technique of RSS based detection along with the procedure of authenticating the node by computing message authentication code (MAC). This approach helped in correct determination of Sybil identity with higher true positive rate.

D. Shehzad et al. [3] gave a new concept for detecting Sybil nodes. He presented a novel mechanism for the detection of Sybil attack in manet. This proposed technique provides assistance in detecting both Simultaneous Sybil and Join and Leave Sybil attacks in network. Hash function mechanism and request threshold validation are the two techniques which are used to serve the purpose of detection.

H.N.Saha et al. [4] proposed a methodology in which he combined two already proposed methods to deal with the Sybil attack. He gave a hybrid solution in which he combined the two techniques named trusted certification and RSSI based solution. This new approach divided the entire network into several subgroups and ensured that each sub group will be monitored by central authority and will also contain RSSI detector nodes. Thus provided a much more practical and efficient solution.

A.Paul et al. [5] in his paper focused on implementing a unique procedure that incorporated combining fuzzy interference rules and neural network based expert system to thwart against Sybil attack. The entire procedure of Sybil attack mitigation is based on trust model. Three phases are involved in its mitigation methodology. In the first phase, behavior of the node is observed thoroughly so as to judge whether it is a Sybil entity. The next two phases involves verifying the case by fuzzy interference and neural network based system.

P.Singh et al. [6] in his paper put forward the concept of Generic Algorithm so as to detect Sybil attackers without relying on centralized trusted third party or additional hardware such as directional antennas. Generic algorithm is a method of soft computing in which the laws of selection and evolution are used.

Balmalthy et al. [7] explained the concept of NDD (neighbor discover distance) algorithm to deal with the sybil attack. These algorithms ensure that data will reach its concerned destination. Passive adhoc identity method and key distribution are used in this method. The procedure of detection can be conducted either by single node or multiple nodes so as to improve the accuracy.

X.LI et al. [8] in his paper has analyzed the security of ElGamal digital signature algorithm under the four attack scheme. He attempted to increase the security of ElGamal algorithm by adding a random number to the original one and thereby creating difficulty in deciphering key.

## 3. SYBIL ATTACK TERMINOLOGY

In Sybil attack, a masquerading hostile entity attempts to pervert the reputation system of a peer to peer network by generating large number of pseudonymous identities. In Sybil attack, a particular node presents more than one identity to the network [9]. The Sybil attack can be conducted by generating fake identities of legitimate nodes. The original identities of legitimate nodes are either captured or the malicious nodes fabricate new identities for themselves [10,11]. Thus a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. The malicious nodes in turn gain control over the decisions of the system, especially if the decision process involves voting or any other type of collaborations. In simple terms, presentation of multiple identities for a single physical node can be termed as Sybil attack.

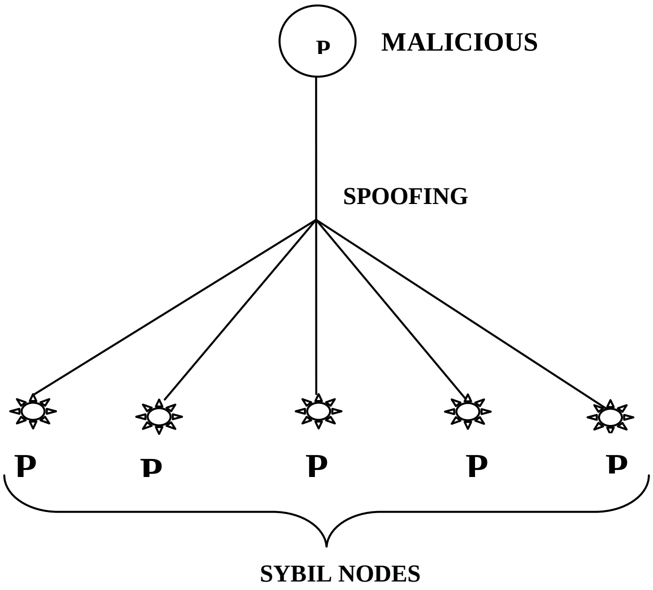

**Fig 1: Sybil Attack**

Figure.1 shows general description of Sybil attack. In the above figure, the node spoofing the identity of the legitimate node is called malicious node or Sybil attacker. The nodes whose identities are spoofed are called Sybil nodes. With respect to the figure, P is the malicious node along with its four Sybil nodes (P1, P2, P3, P4 and P5). Whenever the malicious node tries to interact with any legitimate node by presenting all its identities, the legitimate node will assume that as if it is communicating with five different nodes. But the fact is that there exists only one physical node with multiple identities.

S.Boora et al. [12] presented some adverse effects of Sybil attack:

- Presence of Sybil node may create obstacle in identifying the malicious node.
- Sybil attacks prevent fair resource allocation among the nodes in network.
- Sensors can be used to perform voting for decision making, in few applications. Due to presence of duplicate identities the outcome of voting process may vary.
- Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in the network.

## 3.1 Dimensions of Sybil Attack

There exist three dimensions of launching a Sybil attack. Figure.2 depicts different dimensions of launching a Sybil attack.

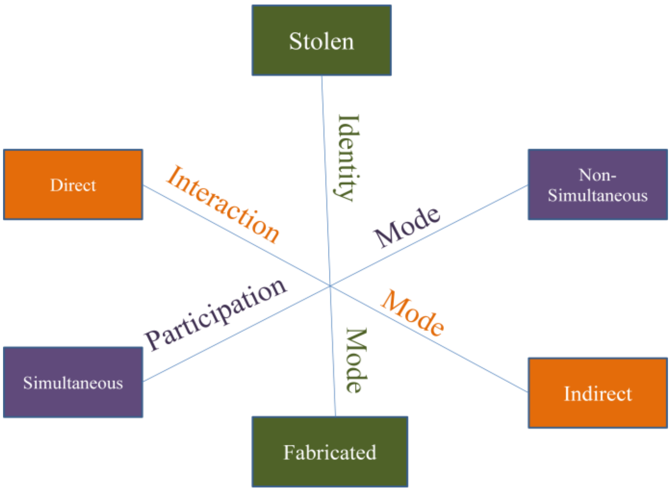

**Fig 2: Dimensions of Sybil attacks**

**Table 1. Dimension modes and their description**

| DIMENSION MODES | TYPES | DESCRIPTION |
|---|---|---|
| INTERACTION MODE | 1) DIRECT COMMUNICATION<br>2)INDIRECT COMMUNICATION | **DIRECT COMMUNICATION**<br>Sybil nodes communicate directly with legitimate nodes.<br>**INDIRECT COMMUNICATION**<br>Legitimate nodes do not interact directly with Sybil nodes. Malicious nodes are used as router by legitimate nodes to reach Sybil nodes. |
| IDENTITY MODE | 1)FABRICATED IDENTITY<br>2)STOLEN IDENTITY | **FABRICATED IDENTITY**<br>Attacker creates arbitrary new identities.<br>**STOLEN IDENTITY**<br>Attacker assigns legitimate identities to Sybil nodes i.e. steal the identity of legitimate nodes. |
| PARTICIPATION MODE | 1)SIMULTANEOUS<br>2)NON-SIMULTANEOUS | **SIMULTANEOUS**<br>Attacker participates with all his identities at once. A malicious node launches all the fake identities at once after the other.<br>**NON-SIMULTANEOUS**<br>Attacker presents large number of identities over a period of time, after fixed or variable interval of time. |

Table .1 presents overall description of dimension modes for launching a Sybil attack.
Thus, in Sybil attack, the attacker basically tries to subvert the system by creating a large number of sybils i.e. pseudonymous identities in order to disrupt normal functioning of the system.

## 3.2 Sybil Attack Mitigation

Figure.3 represents various techniques to deal with Sybil attack in MANET.

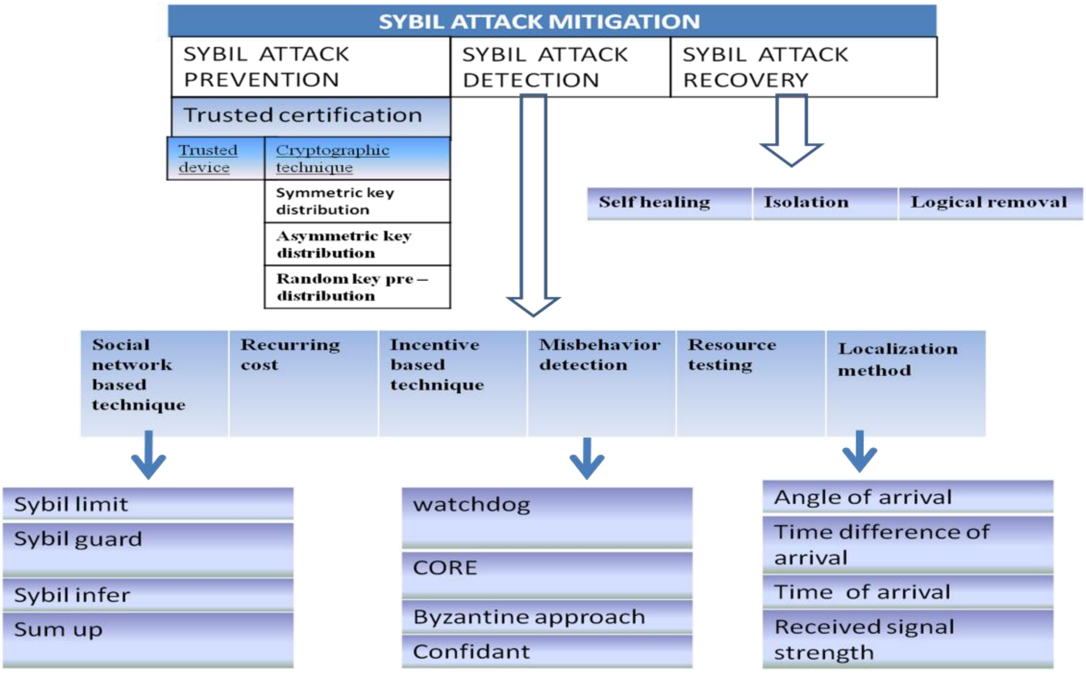

**Fig 3: Sybil attack mitigation**

# 4. RELATED WORK

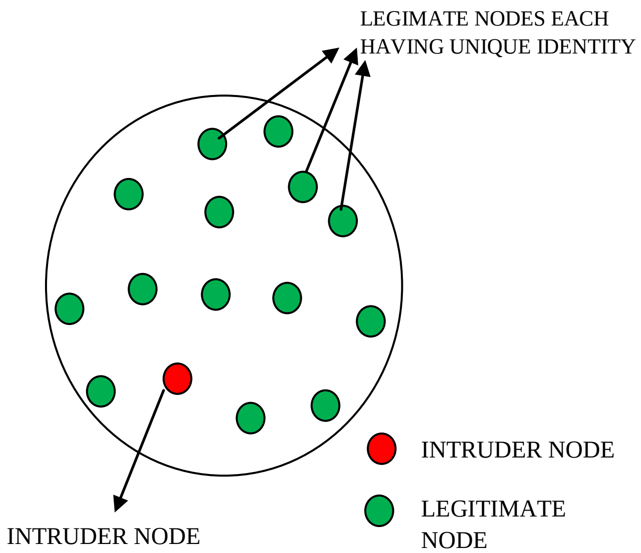

**Fig 4: Simple network comprising nodes**

The above figure.4 depicts a simple network that consists of numerous legitimate nodes each having their unique and distinct identities. Malicious node is present in the network that attempts to disrupt the overall network functionality by creating pseudonymous identities. This intruder node will be termed as Sybil node. This Sybil node tries to forge different identities so as to confuse the network with multiple fake nodes. As there exist single unique identity it becomes easy for the attacker to capture the identity and fabricate new ones. To implement this existing technique ElGamal algorithm has been used as a base.

ELGAMAL ALGORITHM

1. secret key x, public keys α, β, *p*. p is a large prime.
2. Compute $\beta = \alpha^x \bmod p$
   $\alpha^x = \beta \bmod p$ --------> DLP equations
3. Choose a random number k such that $0<k<p-1$ and $\gcd(k,p-1)=1$
   $\gamma=\alpha^k \bmod p$
4. Signature of m is a pair (γ, δ) where $0<= \gamma, \delta<=p-1$
   $\alpha^m=\beta^\gamma \gamma^\delta \bmod p$
   $\alpha^m = \alpha^{x\gamma} \alpha^{k\delta} \bmod p$
   $\alpha^m = \alpha^{x\gamma+k\delta} \bmod p$

message, $m=( x\gamma+k\delta ) \bmod (p-1)$
$\delta=(m-x\gamma)k^{-1} \bmod (p-1)$

verification, $\alpha^m = \alpha^{x\gamma+k\delta} \bmod p$

signature (γ, δ)

## 4.1 Proposed Methodology

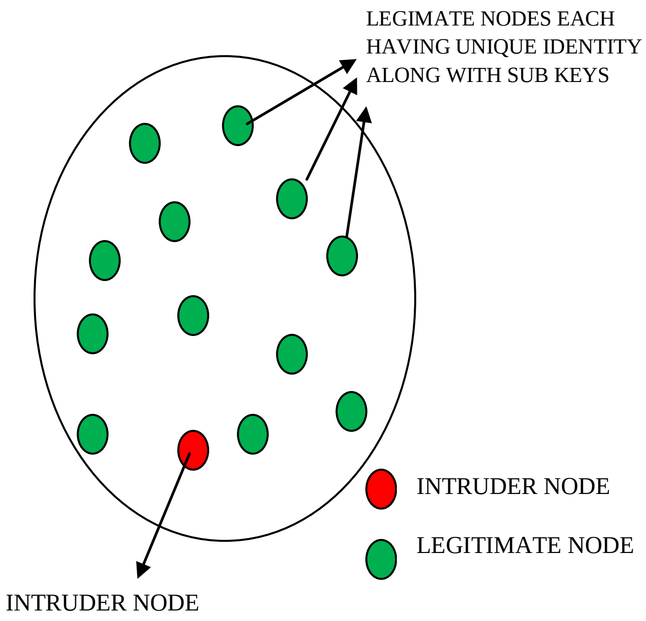
LEGIMATE NODES EACH HAVING UNIQUE IDENTITY ALONG WITH SUB KEYS
INTRUDER NODE
LEGITIMATE NODE
INTRUDER NODE

**Fig 5: Simple network comprising nodes**

The above figure.5 depicts a simple network that consists of numerous legitimate nodes each having their unique identities along with sub keys. These sub keys are chosen randomly. Presence of sub keys makes the system much more secure as compared to the previous one. In this proposed technique, each legitimate node can swap their sub keys (sub identities) after a fixed time period. This swapping will create obstacle for the attacker to fabricate new pseudonymous identities. As the attacker will get confused which key is actually used by the node to forward the message. To implement this technique ElGamal algorithm is used.

Proposed ElGamal algorithm:

1. Private Key a, which is selected by the signer and Public key A, Z, p where p is a larger prime number.
2. So, Compute $A = Z^a \bmod p$, $a(1<a<p-1)$
   $Z^a = A \bmod p$……………DLP equation
3. Choose sub keys (b,c,d,……….z). (These sub keys are chosen randomly).

where, $0<(b,c,d,e,……z)<p-1$
$\gcd((b,c,d,e,……z),p-1) = 1$

with the help of sub keys, we will generate signature values-

$A = Z^a \bmod p$

$$\left.\begin{array}{l} \text{So from sub keys-} \\ B = Z^b \bmod p\ ,\quad 0<b<p-1 \\ C = Z^c \bmod p\ ,\quad 0<c<p-1 \\ D = Z^d \bmod p\ ,\quad 0<d<p-1 \\ . \\ . \\ \text{generation} \\ . \\ . \\ Y = Z^y \bmod p\ ,\quad 0<y<p-1 \end{array}\right\} \text{key + signature}$$

4. Signature of m is a pair(B,C,D,E……..Y)
where $0<=( B,C,D,E……..Y)<= p-1$

NOTE- *Message pair values varies from B to Y. A and Z are not included in this pair because both values have already been used as public keys.*

So, $Z^m = (A^B B^C C^D D^E .............. Y^Z) \text{mod } p$

Since, $A = Z^a$, $B = Z^{b,}$ …………$Y = Z^y$

Therefore, $Z^m = (A^B B^C C^D D^E .............. Y^Z) \text{mod } p$

$Z^m = (Z^{aB} Z^{bC} Z^{cD} Z^{dE} .............. Z^{yZ}) \text{mod } p$

$Z^m = Z^{(aB+bC+cD+dE..............+yZ)} \text{modp}$

Message, $m = (aB+bC+cD+dE…………..+yZ) \text{ mod } (p-1)$

Signature of m is (B, C, D, E,………Y)

Verification , $Z^m = (A^B B^C C^D D^E .............. Y^Z) \text{mod } p$

## 5. CONCLUSION

In this paper emphasis has been laid on preventing Sybil attack using ElGamal algorithm as a base. This paper has presented the concept of swapping the random sub keys that will create obstacle for the hacker to intervene and create new identities. This trick will confuse the hacker as he won't be able to judge which key is actually used by the legitimate node to forward the authenticated message. Even if he succeeds in retrieving any key and he tries to generate pseudonymous identity it will be termed as a big failure because till that time the keys would have been already swapped by the legitimate node or network administrator.

In future, this technique can be further implemented for preventing multiple attacks. Researchers can utilize various cryptographic algorithms to combat such type of malicious attacks.

## 6. REFERENCES

[1] S.lahar," Security in MANET: Vulnerabilities, Attacks & Solutions", International Journal of Multidisciplinary and Current Research,ISSN: 2321-3124 ,Vol.2 (Jan/Feb 2014 issue)

[2] N. Joshi & M. Challa," Secure Authentication Protocol to Detect Sybil Attacks in MANETs", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345, Vol. 5 No. 06 Jun 2014,

[3] D. Shehzad, Dr. A. I. Umar, N. Ul Amin, & WaqarIshaq," A Novel Mechanism for Detection of Sybil Attack in MANETs", International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18, 2014 Dubai (UAE),

[4] H. N. Saha , Dr. D. Bhattacharyya & Dr. P. K.Banerjee , "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack", International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) Volume 1, Issue 4, December 2010

[5] A.Paul, S. Sinha & S. Pal," An Efficient Method to Detect Sybil Attack using Trust based Model", Proc. of Int. Conf. on Advances in Computer Science, AETACS, Elsevier, 2013

[6] P.Singh & R. Bhardwaj, "Prevention of Sybil attacks in manet", International journal of Latest scientific research and technology 1(2),ISSN:2348-9464, July 2014.

[7] Balamalathy.N,Parvathi.S &Kumaresan.A, " AN EFFICIENT METHOD TO DETECT AND PREVENT SYBIL ATTACK", IJCSEC International Journal of Computer Science and Engineering Communications, Vol.3, Issue 2, 2015, Page.685-690, ISSN: 2347–8586

[8] X.Li, X.Shen & H.Chen, "ElGamal Digital Signature Algorithm of Adding a Random Number", JOURNAL OF NETWORKS, VOL. 6,NO. 5, MAY 2011

[9] P.Sharma & D.Dembla,"A Taxonomy of Network Layer Attacks against Wireless Sensor Networks",IJCSC, Vol.4, Number 1 March 2013 pp.81-85 ISSN-0973-7391

[10] C. Diwaker, S. Choudhary & P. Dabas," ATTACKS ON MOBILE AD-HOC NETWORKS",International Journal of Software and Web Sciences (IJSWS), International Association of Scientific Innovation and Research (IASIR), ISSN (Print): 2279-0063 ISSN (Online): 2279-0071

[11] Gagandeep, Aashima & P. Kumar," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Vol.1, Issue-5, June 2012

[12] S. Boora, S. Ohri," A Survey of Layer Specific and Cryptographic Primitive attacks and their countermeasures in Manet's",International Journal of P2P Network Trends and Technology (IJPTT) –Vol.3 Issue4- May 2013