Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Optimisation Techniques against Sybil Attack on MANET

Simranjeet Kaur
Dept.of Computer Science and Engineering
Chandigarh Engineering College
Landran, Mohali, India

Gagangeet Singh Aujla
Dept.of Computer Science and Engineering
Chandigarh Engineering College
Landran, Mohali, India

Sahil Vashist
Dept.of Computer Science and Engineering
Chandigarh Engineering College
Landran, Mohali, India

Abstract—MANET is defined as the "collection of mobile nodes, communicating with each other by the wireless links". It is a challenging chore to achieve security in a Mobile ad hoc network due to its wireless nature, lack of infrastructure and its topology which changes dynamically. Due to its wireless nature there are lots of attacks which can create lots of problems in the MANET. Among various attacks there is a Sybil Attack which is very harmful for mobile ad hoc network. In this attack a malicious node obtain multiple identities at a time and increases lot of misjudgments among the node of the network or it may access the identity of the other legitimate nodes and create false expression of that node in the network. There are a lot of security models and encryption algorithms to secure the network. In this paper two approaches Advanced Encryption Standard (AES) and Rivest Cipher 5 (RC5) are discussed along with a optimization technique that is Genetic Algorithm (GA). In the end it has been proposed that a Hybrid algorithm can be developed that will overcome the limitations of AES and RC5.

Index Terms— MANET, Sybil Attack, AES, RC5, GA.

I. INTRODUCTION

Divergent to infrastructure wireless networks, where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET, does not rely on a fixed infrastructure for its operations. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. Furthermore, devices are free to join or leave the network and they may move randomly and unpredictable topology changes. In this energy-constrained, dynamic, distributed multi-hop environment, nodes need to organize themselves dynamically in order to provide the necessary network functionality in the absence of fixed infrastructure or central administration [1, 2].

Due to MANET'S wireless nature it is exposed to several attacks. Among those attacks there is a Sybil attack which very badly ruins the communication among the nodes of the network. Sybil attack is an attack, in which a malicious node illegitimately claims multiple identities and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. To have secure communication it is necessary to eliminate the Sybil nodes from the network. To prevent the network from the attacks there are many security models and encryption algorithms. The encryption algorithms are of two types symmetric and asymmetric.

This paper is organized as in Section II literature survey will be discussed, in Section III MANET- Architecture, Vulnerabilities, Applications, in Section IV will explain Attacks on Manet, Sybil attack, in Section V Encryption Algorithm, AES, RC5 is explained in Section VI Genetic Algorithm is discussed in Section and Section VII conclusion and future work will be discussed.

II. LITRATURE REVIEW

Kumar et al. [1] discussed about the MANET, history of MANET, application and challenges of MANETS.

Goyal et al. [2] discussed about the vulnerabilities, applications of MANET and fundamental problems of ad hoc network and study how Mobile ad-hoc network bring this technology great opportunistic together.

Stepashkin et. al.(2010) [3] proposed various attacks on MANET. The attacks on Internet connectivity and also on the ad hoc routing protocols. Attacks like DoS, Blackhole attack, Sybil attack, Worm hole attack, Routing attacks etc. and study how different attacks affect the performance of the network.

Piro *et al.* [4] proposed to detect Sybil identities by observing node dynamics. The scheme is discussed which produce high false positives where node density is high or nodes moves in a same direction.

Newsome et al. [5] explain the Sybil attack and its classification and analyzes the threat posed by the Sybil attack to mobile ad hoc networks.

Yu et al. [6] presents a Sybil Guard to prevent the network from the Sybil attack. Sybil Guard exploits this property to bound the number of identities a malicious user can create.

S.William et al. [7] explain the cryptography and encryption techniques. Cryptography is the art of achieving security by encoding messages to make them non-readable. The types of cryptography has been discussed: Symmetric Key and Asymmetric Key.

Karim et al. [8] discussed the various encryption algorithms: DES, RC4 and AES. The comparison has been conducted to process different sizes of data blocks to evaluate the algorithm's encryption/ decryption speed.

Dougles et al. [9] explaining the AES, Advanced Encryption Standard (AES) which is the current standard for secret key encryption as well as the steps of AES algorithm.

Ronald et al. [10] explaining the RC5 encryption algorithm, a fast symmetric block cipher suitable for hardware or software implementations and its various steps.

Thede et al. [11] discussing the optimization technique that is Genetic Algorithm for the optimal solution to a problem and to secure the mobile ad hoc network.

III. MANET

MANET is defined as the "collection of mobile nodes, communicating with each other by the wireless links and making arbitrary graph, using dynamic topology" – with these mentioned characteristic it is very difficult to design any protocol as well as applications for this network [1].

A. Architecture of MANET

There is no such appropriate architecture of MANET due to its wireless nature and other characteristics. While capturing important characteristics, this description does not make explicit how MANETs map into the Internet architecture. Similarly, the lack of a clear architectural description within the context of the Internet has impeded the estimate of the applicability of MANETs within the Internet.

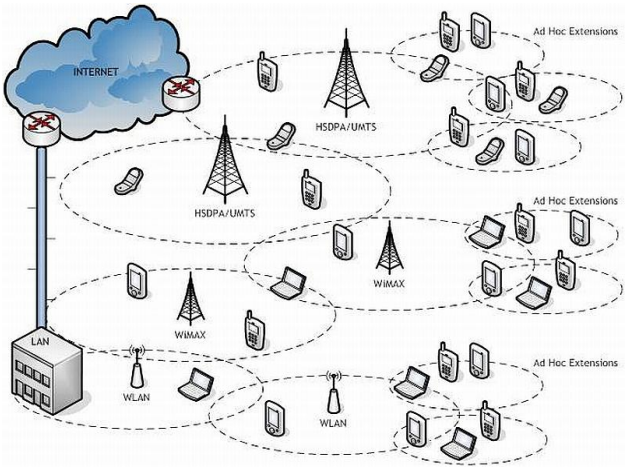


Figure 1: Architecture of MANET

B. MANET Vulnerabilities

Vulnerabilities means weakness in the security system. MANET is more vulnerable then the wired networks. The system may be vulnerable to unauthorized data manipulation because it allow the data access without knowing the user's identity. Some major vulnerabilities are [2]:

- No predefined boundary
- Lack of Centralized Management
- Resource availability
- Scalability
- Limited power supply
- Dynamic topology
- Cooperativeness

C. MANET Applications

As the portable devices are increasing and progress in wireless network is also increased. MANET is gaining importance with the increasing number of widespread applications. The main applications include [2]:

- Commercial sector
- Local level
- Military battlefield
- Personal area network (PAN)

IV. ATTACKS ON MANET

Security in MANET is a major issue. For the better and secure network we must know the possible forms of attacks. So, that we will able to secure our network from that particular attacks. Various attacks on MANET are given below [3]:

Denial of Service attack (DOS): This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

Black hole Attack: In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

Wormhole Attack: In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole.

Replay Attack: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

Snooping: Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.

A. Sybil Attack

Sybil attack was first introduced by J. R. Douceur According to Douceur, the Sybil attack is an attack in which a single entity can control a substantial fraction of the system by presenting multiple identities [4].

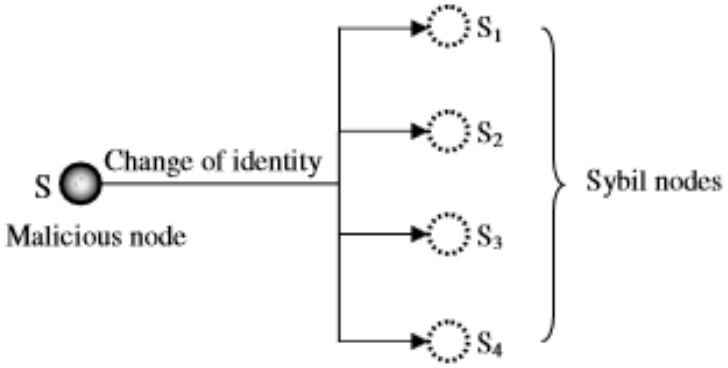


Figure 2: A Sybil Attack with multiple identities.

In a Mobile Ad hoc Network, the only way for an entity to detect the presence of other entities is by sending and receiving the messages over a shared broadcast communication channel. By taking the advantage of this feature, a malicious node can send messages with multiple fake identities. The node spoofing the identities of the nodes is called malicious node/Sybil attacker, and the nodes whose identities are spoofed are called Sybil nodes. Figure 1 represents a malicious node S along with its four Sybil nodes (S1, S 2, S 3 and S4).

B. Sybil Attack Taxonomy

To better recognize the implications of the Sybil attack and how to preserve against it, we develop a taxonomy of its different forms. We propose three orthogonal dimensions as shown in figure 3.

Dimension I: Fabricated vs. Stolen Identities

A Sybil node can get an identity in one of two ways. It can fabricate a new identity, or it can steal an identity from a legitimate node.

Fabricated Identities In some cases, the attacker can simply create arbitrary new Sybil identities. For instance, if each node is identified by a 32-bit integer, the attacker can simply assign each Sybil node a random 32-bit value.

Stolen Identities An attacker don't fabricate new identities and steal the identity of the legitimate node. This identity theft may go undetected if the attacker destroys or temporarily disables the impersonated nodes.

Dimension II: Direct vs. Indirect Communication

Direct Communication One way to perform the Sybil attack is for the Sybil nodes to communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Likewise, messages sent from Sybil nodes are actually sent from one of the malicious devices.

Indirect Communication In this version of the attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed through one of these malicious nodes, which pretends to pass on the message to a Sybil node.

Dimension III: Simultaneous vs Non-Simultaneous

Simultaneous The attacker may try to have his Sybil identities all participate in the network at once. **Non-Simultaneous** Alternately, the attacker might present a large number of identities over a period of time, while only acting as a smaller number of identities at any given time. The attacker can do this by having one identity seem to leave the network, and have another identity join in its place, each device presents different identities at different times.

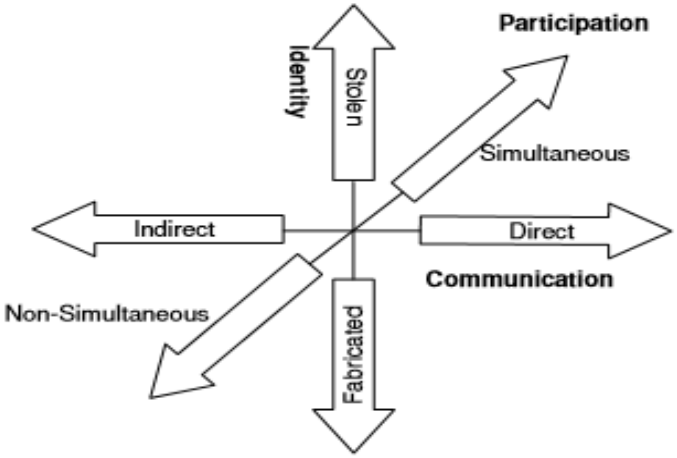
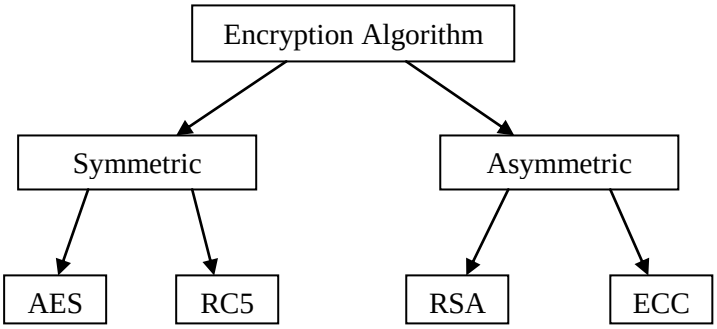


Figure 3. Three dimensions for launching the Sybil attack.

V. ENCRYPTION ALGORITHM

There are number of encryption algorithm which generate private or public keys and encrypt the data, the data which is send from the source to destination. We evaluate that there are two kind of encryption algorithm that is symmetric and asymmetric [7,8].



AES: Advanced Encryption Standard
RC5: Rivest Cipher
RSA: Ron Rivest, Adi Shamir and Leonard Adleman
ECC: Elliptic Curve Cryptography

In the symmetric key algorithm same key is used for encryption and decryption and in the asymmetric algorithm different keys are used for the encryption and decryption. In this review paper we are discussing the symmetric encryption algorithms that is AES and RC5.

A. ADVANCED ENCRYPTION STANDARD (AES)

AES is a symmetric block cipher. This means that it uses the same key for both decryption and encryption. On the 26 November 2001, AES (which is a standarised version of Rijndael) became a FIPS standard (FIPS 197) [9]. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128,192,256 bits. Depending on which version is used, the modified name of the standard are AES-128, AES-192 or AES- 256 respectively.

AES Algorithm

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows[9] :

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage.

SubBytes()

SubBytes() adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

ShiftRows()

ShiftRows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.

MixColumns()

MixColumns() also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics

AddRoundKey()

The actual 'encryption' is performed in the AddRoundKey() function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule.

AES key expansion

The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words. Each round uses 4 of these words. Each word contains 32 bytes which means each subkey is 128 bits long.

The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word w[i] depends on the immediately preceding word, w[i − 1], and the word four positions back w[i − 4]. In three out of four cases, a simple XOR is used. For a word whose position in the w array is a multiple of 4, a more complex function is used. The generation of the first eight words of the expanded key using the symbol g to represent that complex function. The function g consists of the following subfunctions:

1. RotWord performs a one-byte circular left shift on a word. This means that an input word [b0,b1,b2,b3] is transformed into [b1,b2,b3,b0].
2. SubWord performs a byte substitution on each byte of its input word, using the s-box described earlier.
3. The result of steps 1 and 2 is XORed with round constant, Rcon[j].

The round constant is a word in which the three rightmost bytes are always 0. Thus the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j] = (RC[J], 0,0,0), with RC[1]= 1, RC[j]= 2• RC[j − 1] and with multiplication defined over the field GF.

The key expansion was designed to be resistant to known cryptanalytic attacks. The inclusion of a round-dependent round constant eliminates the symmetry, or similarity, between the way in which round keys are generated in different rounds.

B. RC5 Algorithm

The RC5 encryption algorithm was designed by Professor Ronald Rivest of MIT and first published in December 1994 [10].

RC5 algorithm, consists of three components: a key expansion algorithm, an encryption algorithm, and a decryption algorithm. We present the encryption and decryption algorithms first.

Encryption

We assume that the input block is given in two w-bit registers A and B. We also assume that key-expansion has already been performed, so that the array S[0...t−1] has been computed. Here is the encryption algorithm in pseudo-code:

```
A = A + S[0];
B = B + S[1];
for i = 1 to r do
    A = ((A ⊕B) <<< B) + S[2 ∗ i];
    B = ((B ⊕A) <<< A) + S[2 ∗ i + 1];
```

The output is in the registers A and B.

Decryption

The decryption routine is easily derived from the encryption routine.

```
for i = r downto 1 do
    B = ((B − S[2 ∗ i + 1]) >>> A) ⊕A;
    A = ((A − S[2 ∗ i]) >>> B) ⊕B;
B = B − S[1];
A = A − S[0];
```

Key Expansion

The key-expansion routine expands the user's secret key K to fill the expanded key array S, so that S resembles an array of t = 2(r+1) random binary words determined by K. The key expansion algorithm uses two "magic constants," and consists of three simple algorithmic parts [10].

Definition of the Magic Constants The key-expansion algorithm uses two word-sized binary constants Pw and Qw. They are defined for arbi- trary w as follows:

$$Pw = Odd((e - 2)2w) \quad (1)$$

$$Qw = Odd((\varphi - 1)2w) \quad (2)$$

where

e = 2.718281828459..(base of natural logarithms)

φ = 1.618033988749... (golden ratio) ,

and where Odd(x) is the odd integer nearest to x.

Converting the Secret Key from Bytes to Words. The first algorithmic step of key expansion is to copy the secret key K[0...b − 1] into an array L[0...c − 1] of c = db/ue words, where u = w/8 is the number of bytes/word. This operation is done in a natural manner, using u consecutive key bytes of K to fill up each successive word in L, low-order byte to high-order byte . Any unfilled byte positions of L are zeroed. On "little-endian" machines such as an Intel '486, the above task can be accomplished merely by zeroing the array L, and then copying the string K directly into the memory positions representing L. The follow- ing pseudo-code achieves the same effect, assuming that all bytes are "unsigned" and that array L is initially zeroed [8].

for i = b − 1 down to 0 do L[i/u] = (L[i/u] <<< 8) + K[i];

Initializing the Array S. The second algorithmic step of key expansion is to initialize array S to a particular fixed (key-independent) pseudo-random bit pattern, using an arithmetic progression modulo 2w determined by the "magic constants" Pw and Qw. Since Qw is odd, the arithmetic progression has period 2w.

S[0] = Pw; for i = 1 to t − 1 do S[i] = S[i − 1] + Qw;

Mixing in the Secret Key. The third algorithmic step of key expansion is to mix in the user's secret key in three passes over the arrays S and L. More precisely, due to the potentially different sizes of S and L, the larger array will be processed three times, and the other may be handled more times.

i = j = 0;

A = B = 0;

do 3 ∗ max(t,c) times:

A = S[i] = (S[i] + A + B) <<< 3;

B = L[j] = (L[j] + A + B) <<< (A + B);

i = (i + 1) mod(t); j = (j + 1) mod(c);

The key-expansion function has a certain amount of "one-wayness":
it is not so easy to determine K from S.

V1. GENETIC ALGORITHM (GA)

A genetic algorithm is a type of searching algorithm. It searches a solution space for an optimal solution to a problem. The algorithm creates a "population" of possible solutions to the problem and lets them "evolve" over multiple generations to find better and better solutions.

The population is the collection of candidate solutions that we are considering during the course of the algorithm. Over the generations of the algorithm, new members are "born" into the population, while others "die" out of the population. A single solution in the population is referred to as an individual. The fitness of an individual is a measure of how "good" the solution represented by the individual is. The better the solution, the higher the fitness [11].

Algorithm

1. Create a population of random candidates solutions named pop.
2. Until the algorithm termination conditions are met, do the following (each iteration is called a generation):

(a) Create an empty population named new-pop.

(b) While new-pop is not full, do the following:

i. Select two individuals at random from pop so that individuals which are more fit are more likely to be selected.

ii. Cross-over the two individuals to produce two new individuals.

(c) Let each individual in new-pop have a random chance to mutate.

(d) Replace pop with new-pop.

3. Select the individual from pop with the highest fitness as the solution to the problem.

The selection process is analogous to the survival of the fittest in the natural world. Individuals are selected for "breeding" (or cross-over) based upon their fitness values – the fitter the individual, the more likely that individual will be able to reproduce [11].

VII. CONCLUSION AND FUTURE WORK

MANET is a wireless mobile ad hoc network. Due to its wireless nature and lack of infrastructure MANET is vulnerable to various attacks and among them there is a harmful attack that is Sybil Attack. Sybil Attack is an attack in which a malicious node obtain multiple identities at a time and create lot of misjudgment in the network. To have a safe communication network must be secured. In this paper we conclude that AES is much secure encryption scheme as compare to the old private key encryption algorithm and RC5 is even more secure and better than the AES.

For the future work we can provide better output and much secured encryption key by integrating both the algorithms AES and RC5. So, that it will be difficult for the hacker to hack the key. We will propose a Hybrid algorithm with the use

of both AES and RC5. Hybrid algorithm will also be a symmetric encryption algorithm as AES and RC5 both are of same kind. We are proposing this encryption technique for the better security purpose as in MANET we always required much secured network for the safe communication. So, that's why we will make this Hybrid algorithm in the future.

REFERENCES

[1] Mohit Kumar and Rashmi Mishra, "An Overview of MANET" In IJCSE Vol. 3 No. 1 Feb-March 2012.
[2] Priyanka Goyal, "MANET: Vulnerabilities, Challenges, Attacks, Applications" In IJCEM Vol. 11, January 2011.
[3] Mihail Stepashkin," Various Attacks on Mobile Ad-Hoc Networks: an Overview", *ieee(2010)*.
[4] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in *Proc. Securecomm Workshops*, 2006, pp 1–11.
[5] James Newsome, Elaine Shi, Dawn Song and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses" IPSN'04, April 26-27,2004, Berkeley, California, USA.
[6] Haifeng Yu and Michael Kaminsky, "SybilGuard: Defending Against Sybil Attacks via Social Networks" *IEEE*, Vol. 16, No. 3, June 2008.
[7] S. William, Cryptography and Network Security: Principles and Practice , 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.
[8] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms" IJCAT, Vol. 4, No.3, January 2010.
[9] Douglas Selent, " Advanced Encryption Standard" InSight: Rivier Academic Journal, Volume 6, Number 2, Fall 2010.
[10] Ronald L. Rivest, "The RC5 Encryption Algorithm"
[11] Scott M.Thede, "An Introduction to Genetic Algorithm" IN 46135, JCSC 20, 1 (October 2004).

