EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.92-98
SANA ACADEMIC PRESS

Revealing of join acting up using Overhearing and self-governing Agents using ECC algorithm in Wireless improvised Networks

Aruna G M[1], R.Latha[2]
[1]Research Scholar, St. Peter's University, Chennai.7
[2]Prof. & Head., Dept. of Computer Applications, St. Peter's University, Chennai
gmmmaruna@gmail.com

Abstract - *Mobile Ad Hoc Network (MANET) is formed by a set of wireless mobile hosts that dynamically configure themselves by exploiting their wireless network interfaces without relying on any fixed infrastructure. Mobile hosts used in MANET supports the roles that are ensured by the powerful fixed infrastructure in traditional networks. This is a challenging task for the mobile hosts that have limited resources such as processing power, storage and energy. Misbehavior is defined as an unauthorized behavior of an internal node that results unintentional damage to other nodes. The aim of the node is not to launch an attack but it may have other aims such as obtaining an unfair advantage compared with the other nodes. For instance, one may not correctly execute the MAC protocol with the intent of getting higher bandwidth or it may refuse to forward packets for others to save its resources, while using their resources and asking them to forward its own packets. The mobile hosts that are not directly connected can communicate by forwarding their traffic via a sequence of intermediate mobile hosts. In existing a neighbor Overhearing based Misbehavior Detection (OMD) scheme was presented. And also Autonomous Agent based Misbehavior Detection (AAMD) technique was presented. This paper present a Path tracing algorithm to detect the malicious attack using per hop distance and pixel wise measurements link frequent appearance count parameters using AODV. The simulation results of the proposed scheme shows a promising result in the measured parameters when compared to the existing neighborhood monitoring based overhearing method and to protect the Received project from the hackers or attackers, we use ECC algorithm.*

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on pre-existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. All network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves either individually or collectively. The mobile hosts that are not directly connected can communicate by forwarding their traffic via a sequence of intermediate mobile hosts. In existing a neighbor Overhearing based Misbehavior Detection (OMD) scheme was presented. And also Autonomous Agent based Misbehavior Detection (AAMD) technique was presented.

This project present a Path tracing algorithm to detect the malicious attack using per hop distance and pixel wise measurements link frequent appearance count parameters using AODV. There are two types of MANETs: closed and open. In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/rescue or military and law enforcement operations. Identification of misbehaving nodes in ad hoc networks is critically important to detect security attack in the network. Two types of misbehaving nodes such as selfish and malicious nodes are taken into consideration. Selfish nodes do not intend to directly damage other nodes, but however, do not cooperate, saving battery life for their own communications. But malicious nodes do not give priority to saving battery life, and aim at damaging other nodes. It is introduced that two different types of selfish nodes. As the nodes in MANETs are battery powered, energy becomes a precious resource, and thus, role of selfish nodes draws more attention.

A. Type-0: well-behaved node

A well behaved node cooperates in the communication well, performs as required by the routing protocol, and equally participates in the communication activities like route discovery, maintenance, packet forwarding and receiving etc.

B. Type-1: active selfish node

Such a node does not participate in packet forwarding, and drops every received packet. It disables the packet forwarding mechanism for the packets which have a destination address, other than this selfish node. It helps the selfish node to save its own energy, thereby still contributing to network maintenance.

C. Type 2: passive selfish node

Such a node practically does nothing and stays idle in the network. It does not contribute to any of the activities like packet forwarding, receiving, route discovery, network maintenance. Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes. Selfish nodes can severely degrade network performance and eventually partition the network by simply not participating to the network operation. There are four types of misbehaviors in ad hoc networks,

- failed node behaviors,
- badly failed node behaviors,
- selfish attacks, and
- malicious attacks

2. EXISTING SYSTEM

Nodes in mobile ad-hoc network are highly mobile which causes network topology to change rapidly at unpredictable times. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. So it’s making data transition problem. Another Problem it will drop more dropping packets, making time delay, reduce delivery ratio, as well as throughput because of misbehave node.

Disadvantage

- Packet drop out
- Large no. of packet’s are wasted
- Delay time of node is very high
- Detection time of the misbehave node will take more time on the particular time
- Packet delivery ratio is very low on existing system
- False misbehavior and partial dropping is difficult

3. PROPOSED SYSTEM

The focus of the work is implementing and finding the dropping packets for optimal estimation for AODV. Path tracing algorithm to detect the malicious attack using per hop distance and pixel wise measurements link frequent appearance count parameters using AODV. So it can detect accurate misbehave person. There is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

MANET Architecture diagram

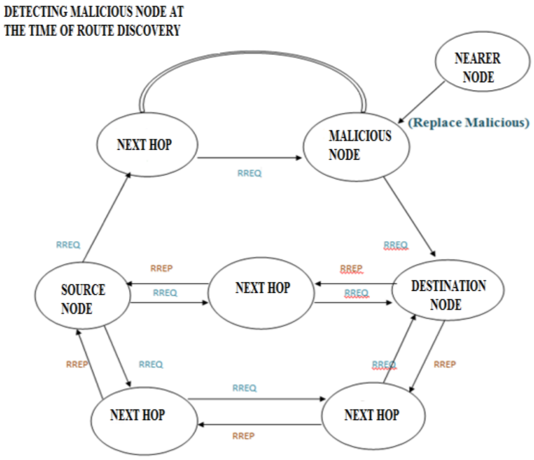

Fig.1. Architecture diagram

Advantages

- The pause time variations with control packets, packet delivery ratio, and end-to-end delay, are taken into consideration for the mobility of the nodes in the network

- The algorithms used should be simple, and also it should be ensured that they do not lead to high computational and storage cost
- The constant bit rate (packets per second) variations provide the best accuracy packet delivery

4. METHODOLOGY

- AODV Route Discovery
- Misbehavior Detection
- Misbehavior Isolation
- ECC Implementation

1) AODV Route Discovery

AODV algorithm is made used here. The 3 methods are RREQ, RREP, RERR with the Acknowledgement gained AODV finds the right path with Shortest distance. It takes into account only the nearby node. It transfers the packet to that Discovered Node. Whenever an AODV router receives a request to send a message, it checks its routing table to see if a route exists.

2) Misbehavior Detection

This work focuses on detecting the misbehaviour using OMD and AAMD algorithm. This algorithm only detects the misbehaviour on the particular area. Find out process on the backend.

3) Misbehavior Isolation

To detect misbehaviour fast using path tracing algorithm, and to helps in eliminating the misbehaviour on the path.

4) ECC implementation

ECC algorithm is used to effectively transfer data packets from source to destination and helps in enhancing the security of authentication.

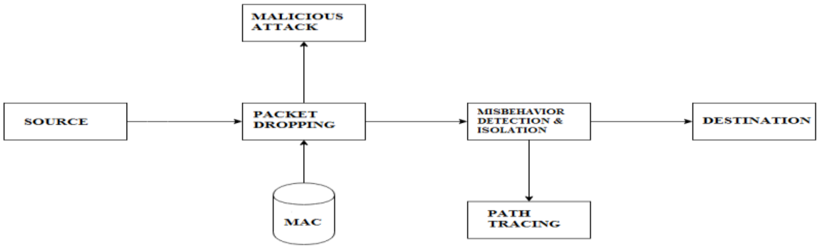

Fig. *2. Misbehavior Detection and Misbehavior Isolation*

a) ECC Algorithm

1) For secure data transmission we use Elliptic Curve Cryptography algorithm which uses key generation technique
2) The sender will encrypt the message with receiver's public key and the receiver will decrypt its private key.
   Q = d * P generates the public key

Where d = the random number that we have selected within the range of (1 to n-1).P is the point on the curve. Q is the public key d is the private key.

ECC (Elliptical Curve Cryptography)

Elliptical curve cryptography (ECC) is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been developing its own version of ECC.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

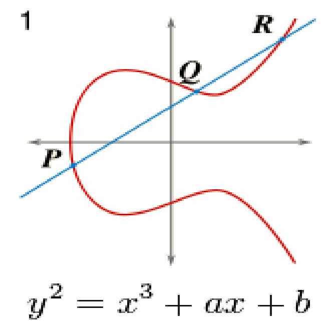

Fig. 2. Simple elliptic curve

- **Encryption**

Let ‘m’ be the message that we are sending
Consider *‘m’* has the point *‘M’* on the curve *‘E’*.Randomly select ‘k’ from [1 - (n-1)].
Two cipher texts will be generated let it be **C1** and **C2**.

$C1 = k*P$

$C2 = M + k*Q$

C1 and C2 will be sent.

- **Decryption**

We have to get back the message ‘m’ that was sent

$M = C2 – d * C1$

M is the original message that we have send.

Work Done

$M = C2 – d * C1$

‘M’ can be represented as ‘C2 – d * C1′

$M=C2 – d * C1$

$= (M + k * Q) – d * (k * P)$

(C2 = M + k * Q and C1 = k * P)

= **$(M + k * (d * P)) – d * k *P$**

$= M + (k*d*P)-(d*k*p)$

(Q=d*P) (Cancelling out k * d * P)

= M (Original Message)

Source node encrypts the message using ECC algorithm. The encrypted message is transferred in data packets along the randomly selected path. Other nodes cannot see what is being transferred in the packets. Once data packets reached the destination, data’s are decrypted in the destination node using the cipher key. Message sent from source is received in destination without loss or damage to data.

b) Performance Evaluation

- Packet delivery ratio
- Delay
- Average delay
- Throughput

5. FUTURE ENHANCEMENT

Video transmission over MANETs is more challenging than over conventional wireless networks due to rapid topology changes and lack of central administration. Misbehaving nodes that exhibit abnormal behaviors can disrupt the network operation and affect the network availability by refusing to cooperate to route packets due to their selfish or malicious behavior. So that in future projects we can examine the effect of packet dropping attacks on video transmission over MANETs.

6. CONCLUSION

The focus of the work presented the security level of wireless Mobile Ad hoc Networks with greater packet delivery ratio, lesser end to end delay, lesser control overhead, and lesser energy consumption requirement, by introducing and analyzing the concept of the path tracing algorithm. It also obtain a strong resilience against node capture and high connectivity with highly secured nodes, based on trust, and to establish an authenticated route thereby enabling secure data transfer. This scheme introduced a novel dynamic acknowledgment ratio to make the nodes to request its second hop successor in the source route to acknowledge the receipt of the packet. This makes the nodes to detect the behavior of the next hop links and to select the trusted routes for its transmissions. The misbehaving link information is shared with the rest of the nodes in the network by piggybacking it in the route discovery packet without incurring additional control overhead. And provide security to all packets by using ECC. The performance of this scheme is compared with the neighborhood monitoring based existing scheme. Mobile ad hoc networks (MANET) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. AODV protocol itself incurs a low checking overhead. Path tracing algorithm to detect the malicious attack using per hop distance and pixel wise measurements link frequent appearance count parameters using AODV. So we can detect accurate misbehave person. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

REFERENCES

1) Agarwal, D., & Rout, R. R. (2015, February). Detection of node-misbehavior using overhearing and autonomous agents in wireless Ad-Hoc networks. In*Applications and Innovations in Mobile Computing (AIMoC), 2015* (pp. 152-157). IEEE.

2) Q. Li and G. Cao, “Mitigating Routing Misbehavior in Disruption Tolerant Networks,” IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.

3) S. Samreen and G. Narasimha, “An efficient approach for detection of node misbehavior in a manet based on link behavior,” *IEEE International Journal of Advance Computing Conference*, pp. 588–592, 2012.

4) Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay-Tolerant Networks,” Proc. IEEE INFOCOM ’10, 2010.

5) S. Marti, T.J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile ad-hoc Networks,” Proc. ACM.