International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 12 (2018) pp. 10702-10706

A Security for MANET Interruption Recognition & Preclusion approaches for Network Layer Attacks

V. Nancy
M.Tech, Computer Science Engineering, Department, SRM University, Kattankulathur , Tamil Nadu.

Abstract

Ad hoc networks have the trust factor present among their entities in routing operations. As wireless networks work on limited nodes, it is important for the nodes to cooperate and communicate with the neighboring nodes to extend the network with the remote nodes. In this paper we involve in the trust factor as a solution for OLSR protocol. This approach is suitable for Adhoc networks. The trust factor among the entities makes them to reason out and take decisions depending on the entities. In this research we propose a prototype called the Trust- OLSR (TOLSR) which is based on cooperation and routing operation and attacker detection and prevention. The technique and its contribution and explained in detail in trust-based security in OLSR. A trust based analysis is held for OLSR protocol using trust specification language and we demonstrate how trust based reasoning enables to evaluate the behaviour of the other nodes. Using this method we will detect the misbehaving nodes and then we propose solutions to prevent and counter measure the problem and resolve the situation of inconsistency. We also offer cryptography based security algorithm.

Keywords: TOLSR, ECC, MANET, OLSR

INTRODUCTION

MANET- Mobile Adhoc Network is a self organized communication mode with mobile nodes and without a central coordinator. The node in the MANET can be any mobile device that has the ability to communicate with other nodes. The nodes in the MANET network work as both as a host and as a router. The unique feature of MANET over traditional methods is its ease to be set up and destroyed and also the flexible nature of the nodes. Optimized Link State Routing (OLSR) protocol is a commonly used algorithm today. OLSR is efficient in using the bandwidth and in path calculation but it is vulnerable to attacks. Since this prototype is dependable on the cooperation between network nodes it is easy to confuse rogue nodes and at times even a single malicious node can destroy the entire network set up. The possible attacks on OLSR are flooding attacks, spoofing attacks, black-hole attacks, colluding mis-relay attacks and DOS attacks.

In this paper we involve in the trust factor as a solution for OLSR protocol. This approach is suitable for Adhoc networks. The trust factor among the entities makes them to reason out and take decisions depending on the entities. In this research we propose a prototype called the Trust- OLSR (TOLSR) which is based on cooperation and routing operation and attacker detection and prevention. The technique and its contribution and explained in detail in trust-based security in OLSR. A trust based analysis is held for OLSR protocol using trust specification language and we demonstrate how trust based reasoning enables to evaluate the behaviour of the other nodes. Using this method we will detect the misbehaving nodes and then we propose solutions to prevent and counter measure the problem and resolve the situation of inconsistency. We also offer cryptography based security algorithms like ECC security algorithm. ECC delivers tremendous speed and efficiency and many researchers say that it is never been defeated. We improve the existing encryption and decryption techniques and deliver excellent security.

Manet

With a lot of portable devices around us it is important to have a speed and secured wireless communication. For this purpose we need to implement ad-hoc networking to a widespread of applications. Ad-hoc as the name terms it all that this network can be set up anywhere with little or no communication infrastructure. Ad-hoc networks are so scalable that adding and removing a device from the network is easily done without altering the network performance. MANET is applied to several applications which ranges from mobile, large-scale, static networks and small networks. Apart from the traditional applications moving or migrating to the Ad-hoc environment there are a whole set of new services that are supported by MANET.

Its application includes various sectors that are described below. Military Battlefield: Several military equipments are embedded with sensor devices that allow GPRS and UMTS. Adhoc network is best suitable for military as it can form small network technology between vehicles, soldiers and military information headquarters. The concept of Adhoc actually came into picture in military field. Commercial Sector: Adhoc can be used in case of emergency situations like flood, fire, earth-quake etc. In such emergency cases the existing networks will be collapsed or damaged and hence a adhoc network needs to setup. Information will be transformed from one team to another team through palmtop computers, notebook computers and other mini devices. Adhoc network can also be implied on home networks where private devices can be connected. This can be applied for sports stadium, taxicab, aircraft, boat and several other applications. Personal Area Network (PAN): Personal devices like laptop, cellular phone, PDA can be intercommunicated using MANET. In such cases wires are replaced with wireless connections and simplify the network. Other technologies like Wireless LAN (WLAN), UMTS and GPRS can also be used. MANET-VoVoN: In this MANET is enabled with JXTA peer-to-peer, open platform, modular for supporting user

location and audio streaming through JXTA virtual overlay network. This technology uses private signaling protocol based on exchange of XML messages over MANET-JXTA communication channels.

RELATED WORK

D. Dhillon et al [4] proposes an algorithm with PKI implemented with OLSR MANET in the network layer level. The OLSR control packets are used in this method to support various security activities. A fully distributed CA (Certificate Authority) is used in this method and integrated with an existing implementation of OLSRv4 (OLSR for IP version 4).

Yih-Chun Hu et al [2] proposes the wormhole attack in MANET. This attack is the most severe attack in ad hoc networks and it can attack even if the attacker has not compromised any hosts and even if there is authenticity and confidentiality in all communications. In the wormhole attack the attacker records the packets at one location, tunnels them to another location and retransmits them there into the network. The wormhole attack can cause severe damage to ad-hoc networks and also in location-based wireless security systems.

Bounpadith Kannhavong,et al [5] experiments a new routing attack called the Node Isolation attack against the Optimized Link State Routing (OLSR) protocol. The attack is studied in detail through experimental results to show the requirement to find counter measures to protect the network against the attack. A simple technique is proposed by the author as a first step to defense and identify the source of attack.

M. Wang, L. Lamont et al [3] introduces threats to the OLSR MANET routing protocol and also proposes a solution based on protocol semantics checking. This approach is based on the semantic properties and specifies the correct OLSR routing update behaviour. When any abnormal protocol semantics are found it triggers an intrusion alarm. The OLSR can be applied on Multi-Point Relay (MPR) proactive MANET protocol.

Danny Dhillon et al [6] implement the Intrusion Detection System (IDS) where each node in the MANET evaluates the non-conformances locally. After which the possible attacks are found in the routing protocol. The effectiveness of IDS is measured in terms of false positive and false negative detection rates. Though the concept is based on OLSR it can be implemented on any link-state routing protocol.

Mawloud Omar et al [9] provide a trusted model especially for mobile adhoc networks.

In this paper the author discusses about a fully distributed public key certificate management system that's based on trust graphs and threshold cryptography.

It allows the user to issue public key certificates and also process authentication using certificates' chains even without centralized management authorities.

With the concept of threshold cryptography we can even fight against false public keys certification.

Evaluation of the complete approach is tested using simulations.

The outcome shows that the proposed method provides effective security.

Sonal et al [10] proposed a solution for packet loss and data rate against black hole attack in network. This method will initially detect the black hole attack with the help of fuzzy logic and it is also applied on packet loss and data rate during the time of node communication. In this situation it will send the packet using other surrounding nodes. This algorithm can provide better solutions than the other existing methods.

Devesh Malik et al [14] introduces Energy efficient routing algorithm for adhoc networks. This method tries to solve the problem of node isolation in OLSR by altering the existing OLSR. This approach gives more security and also helps in energy conservation problem. This newly formed method is named as DFOLSR.

Mohanapriya Marimuthu et al [15] introduce enhanced OLSR called the EOLSR protocol that works on a trust based technique to secure the OLSR nodes from attacks. This method can authenticate if the node is sending the correct information by verifying the Hello packets. The simulation results show that this protocol can achieve routing security with 45% increase in packet delivery ratio and also 44% reduction in loss of packet. This approach does not involved high computational complexity for securing network.

MATERIALS AND METHODS

We introduce Trust-OLSR (TOLSR) protocol that based on routing and cooperation operation and attacker detection and prevention. The entire technique is designed on trust based security in OLSR. This trust based analysis of OLSR is performed using trust specification language and we also discuss on how trust-based reasoning can help in executing trust-based reasoning suing behaviour of the nodes. After analyzing the mis-behaviour of the nodes we construct a solution for the prevention and counter measures for the attacks. A cryptography based security mechanism is used in this approach called the ECC security algorithm. ECC is well known for its tremendous speed and effectiveness. Improvisation on an existing algorithm through encryption and decryption enhances the existing algorithm performance.

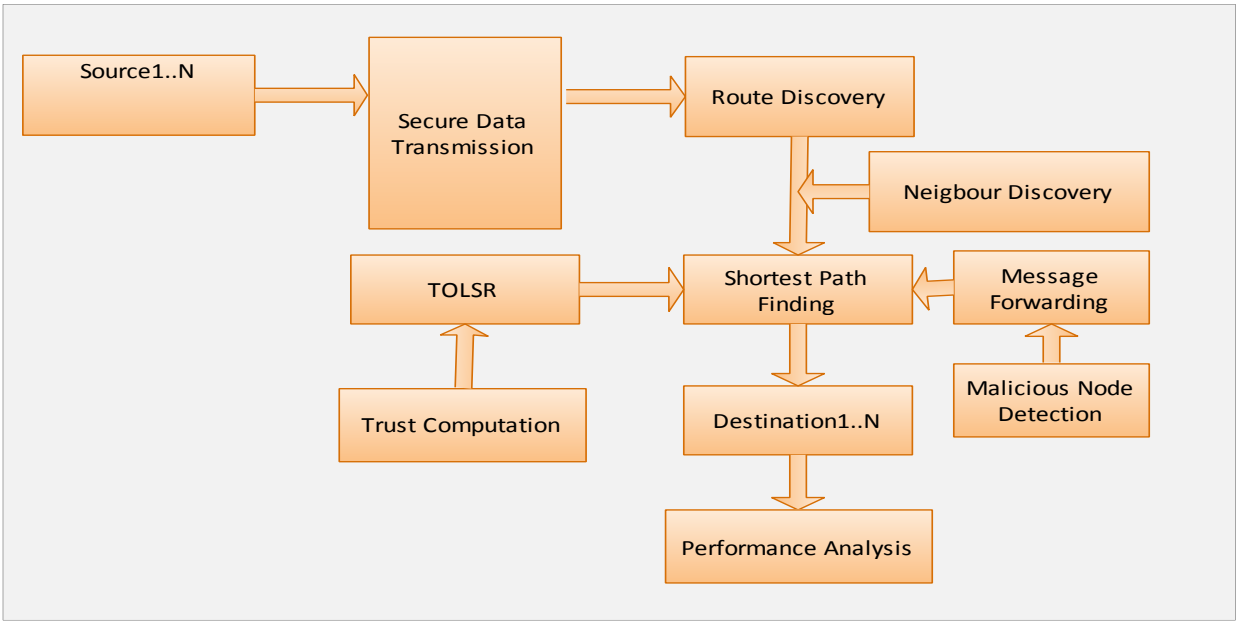

Figure 1. System Architecture

ELLIPTIC CURVE: Some Definitions

Elliptic curve cryptography (ECC) is the most efficient cryptography method in use. We can discuss about the two important eras in the history of cryptography: classical era and the modern era. In 1977, during the introduction of Diffie-Hellman key and the RSA algorithm, modern cryptography came into picture. The concept of declaring the key that is used for encryption as public key and the key used for decryption as private key. In 1985, cryptographic algorithm was formed on the basis of esoteric branch of mathematics called elliptic curves. In this proposed paper we use elliptic curve algorithm for encryption and decryption of data received from sensor nodes.

Scalar Multiplication: Let, k and P be the given integer that lies on the elliptic curve. Then the elliptic scalar multiplication kP is the result of adding Point P to itself k times.

Order: The order of a point P is defined as the smallest integer r where rP= 0. With c and d as integers then cP = dP iff c ≡ d (mod r).

Curve Order: Curve order is the number of points that lies on the elliptic curve and is denoted as #E.

ELLIPTIC CURVE EQUATION

Let's consider an elliptic curve F_p, then the points that satisfy the "curve equation" is:

$$y^2 = x^3 + ax + b \mod p$$

Here, a, b, x and y are within the curve F_p in other words they are the integers modulo p.

The coefficients a and b are called as the characteristic coefficients of the curve and they determine the points that will fall on the curve. The curve coefficients should satisfy the below condition:

$$4a^3 + 27b^2 \neq 0$$

Curve Cryptosystem Parameters

Now, all the discussed mathematical concepts are to be converted into a cryptosystem and for which there must be sufficient parameters to perform the operation. There are 6 distinct values of Fp to determine the domain parameters.

1. p: is a prime number that defines the field where the curve operates, Fp. All the points taken into account will have modulo p. a, b: The two coefficients which define the curve. These are integers.
2. G: is called the generator or base point. It is that distinct point on the curve that defines the start of the curve. This is provided as G or as two points called g_x and g_y
3. n: it is order of the curve generator point G. It is the number of different points on the curve that can be manipulated by multiplying a scalar with G. This value is required only for digital signing using ECDSA the operations are congruent modulo n, not p.
4. h: is the cofactor of the curve and is the quotient of the number of curve-points or #E(F_p), divided by n.

Elliptic Curve Cryptography

1. ECC is based on the hardness of discrete logarithm problem.
2. Consider P and Q as any two points on the elliptic curve satisfying the condition, kP=Q.
3. Here k is a scalar and it is complex to find k when P and Q are provided.
4. k is the discrete logarithm of Q to the base P.
5. Point operation is the main operation to be performed.
6. The scalar k is multiplied with p, k*p in order to achieve another point Q.

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM SIGNING

For signing a message m by sender A, using A's private key d

1. Calculate e = HASH (m), where HASH is a cryptographic hash function, such as SHA-1

2. Select a random integer k from [1,n − 1]

3. Calculate r = x1 (mod n), where (x1, y1) = k * G. If r = 0, go to step 2

4. Calculate s = k − 1(e + dr)(mod n). If s = 0, go to step 2

5. The signature is the pair (r, s)

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM VERIFICATION

In order to authenticate A's signature from B, B must contain A's public key Q.

1. r and s must be integers in [1,n − 1]. If this does not satisfy then the signature is invalid.

2. Calculate e = HASH (m)

3. Calculate w = s −1 (mod n)

4. Calculate u1 = ew (mod n) & u2 = rw (mod n)

5. Calculate (x1, y1) = u1*G + u2*Q 6. The signature is valid if x1 = r(mod n)

GENERATION OF KEY

Generation of key is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number'd' within the range of **'n'**.

Using the following equation we can generate the public key

Q = d * P

'd 'is 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 and **'d'** is the private key.

ENCRYPTION

Let 'm' be the message that we are sending. We have to represent this message on the curve. These have in-depth implementation details.

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 send.

DECRYPTION

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

PROOF

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P)

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

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message)

RESULTS AND DISCUSSIONS

TOLSR uses optimized flooding mechanism to send partial link state information to all network nodes. It is a proactive link-state routing protocol. TOLSR uses multi-point relays (MPR) where selected nodes forward the broadcast messages during the process of flooding. This link state information will be generated only by those that are selected as MPRs. The selected MPRs should only broadcast the state of links between the selector and itself. There are two messages used in this topology namely: HELLO and TC- Topological Control. These messages allow each node to obtain and declare network topology information. These two messages have validity time that indicates how long the information can be considered.

The functionality of TOLSR can be described in three steps: neighbourhood discovery, MPR selection and Routing table calculation. The trust relationship is also estimated between the TOLSR nodes. This trust analysis helps in identifying the

trust assumption in different steps of the protocol and how it can be used by the attackers.

CONCLUSION

We proposed a network called the TOLSR in which hop-by-hop or end-to-end will provide reliability. The main objective of this research is to explore the various ways of encryption. Utilise the existing methods and improvise them with few aspects to create reliability and strong security. These various features can be implemented on different large scale networks to study the security offered. Encryption is done using the AES-Advanced Encryption standard and ECC- Elliptic Curve Cryptography.

REFERENCES

[1] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks", 0-7803-7406-1/01/$17.00©2001 IEEE

[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks", 0733-8716/$20.00 © 2006 IEEE

[3] M. Wang, L. Lamont, P. Mason, M. Gorlatova, "An Effective Intrusion Detection Approach for OLSR MANET Protocol",0-7803-9427-5/05/$20.00© 2005 IEEE

[4] D. Dhillon, T. S. Randhawa, M. Wang, L. Lamont,"Implementing a Fully Distributed Certificate Authority in an OLSR MANET", WCNC 2004 / IEEE Communications Society

[5] Bounpadith Kannhavong, Hidehisa Nakayama, Abbas Jamalipour ," Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks", 1-4244-0491-6/06/$20.00©2006 IEEE

[6] Danny Dhillon , Jerry Zhu, John Richards , Tejinder Randhawa ,"Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada. Copyright 2006 ACM 1-59593-306-9/06/0007...$5.00.

[7] Daniele Raffo , C´edric Adjih "An Advanced Signature System for OLSR", SASN'04, October 25, 2004, Washington, DC, USA. Copyright 2004 ACM 1581139721/ 04/0010 ...$5.00.

[8] P. Suresh, R. Kaur, M. Gaur, and V. Laxmi, "Collusion attack resistance through forced mpr switching in olsr," in Proc. Wireless Days, Oct. 2010, pp. 1–5.

[9] A. Nadeem and M. Howarth, "Protection of manets from a range of attacks using an intrusion detection and prevention system," Telecommun. Syst., vol. 52, no. 4, pp. 2047–2058, 2013.

[10] A. Nadeem and M. P. Howarth, (2014). An intrusion detection & adaptive response mechanism for manets. Ad Hoc Netw. [Online]. vol. 13, pp. 368–380. Available: http://www.sciencedirect.com/ science /article/pii/S1570870513001959

[11] A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2027 2045, Oct.-Dec. 2013.

[12] D. Raffo, "Security schemes for the olsr protocol for ad hoc networks," Ph.D. thesis, Universit_e Paris, 2005.

[13] [Online]. Available: http://www.nsnam.org/, Oct. 2013.

[14] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004.

[15] B. Kannhavong, H. Nakayama, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE trans. Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.