International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017
ISSN 2229-5518

Encryption and Decryption Scheme for Secure Routing Adhoc Network

M.Angelin Rosy, K.Saralasri & R.Rajeshwari

ABSTRACT

A recent trend in accidental network routing is that the reactive on-demand philosophywherever routes aren't established onlyneeded. Most of the protocols during this class aren't incorporating correct security measures. The accidental setting is accessible to each legitimate network users and malicious attackers. It's been discovered that totally different completely different protocols want different methods for security. The key problems regarding these areas are self-addressed here. The cryptic algorithmic program has been planned during this paper. This theme will build most of the on-demand routing protocols secure. The study can facilitate in creating protocols additional study against attacks and standardize parameters for security in protocols. Accidental networks use mobile nodes to alter communication outside wireless transmission vary. Attacks on accidental network routing protocols disrupt network performance and responsibility.

Keyword: Ad hoc network, routing, security, mobile network, mobile application

1. INTRODUCTION

Ad hoc network is a set of wireless mobile nodes form a dynamic network without the intervention of centralized access points or base stations. Ad hoc networks require no fixed network infrastructure and can be deployed as multi hop packet networks rapidly with relatively low expense networks can be very useful in scenarios where natural conditions or time constraints make it impossible to pre-deploy infrastructure [1]. Mobile nodes in an ad hoc network have limited radio transmission range. Nodes that are unable to communicate directly with each other require that intermediate nodes forward packets. Each node acts router and host. The function routing protocol in ad hoc network is to routes between different nodes. Here without network coding, each message would require four transmissions, as shown in fig. 1(2).

Without considering the energy required for encryption and decryption operation, it would save ¼ energy For example, in battle field or in a police van data communicated between vehicles should keep confidential during transmission [1]. The encryption schemes use for providing confidentiality in VANET are not efficient.

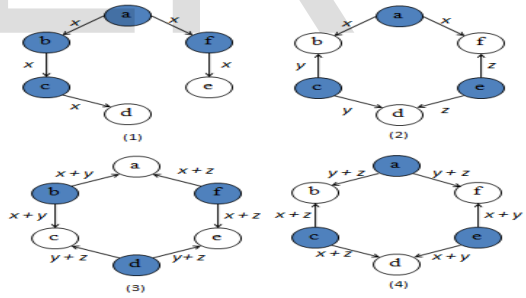

Fig.1 Use of network coding for transmission. Shaded nodes are those involved in transmission.

2. LITERATURE REVIEW

Related work PAMAS

In [5] paper, S. Singh proposes PAMAS protocol for reducing energy consumption. In an ad hoc network, the radio channel is shared by all nodes. That is, when a node transmits data to a specific node, all other node turn them off till the transmission completes. Therefore author propose a power aware protocol called PAMAS which saves energy by turning off nodes not participating in communication.

Node-join-tree

M. Anjelin Rosy, Assistant Professor, Department of Master of Applications(MCA),Er.Perumal Manimekalai College of Engineering,Hosur,Tamil Nadu.

K. Saralasri, Second Year MCA, Er.Perumal Manimekalai College of Engineering,Hosur, ,Tamil Nadu.

R.Rajeshwari, Second Year MCA, Er.Perumal Manimekalai College of Engineering,Hosur,Tamil Nadu.

In [6] paper, author discuss the problem that, in ad hoc wireless network and a multicast request, there is a need to find multicast tree which consumes minimum energy. The author proposes node-join-tree (NJT), which is implemented in distributed fashion.

Random Linear Network Coding

Network Coding used in ad hoc wireless network allows intermediate node not only to store and forward packet but also process and mix different incoming packets. In [7] author proposes a random linear network coding (RLNC) which provides security as well as the advantage of reduced computation or space overhead. Confidentiality can be achieved by locking the source coding vector required to decode the encoded packet, without interrupting the intermediate node from running their network coding operation.

Homo morphic Encryption Function

In [9] paper, author proposes an efficient Homo morphic encryption operation (HEF) perform on Global Encoding Vector which offer privacy-preserving features, like un-traceability and message content confidentiality. This scheme uses random linear coding, where each sink node invert the GEVs to recover.

3. SECURITY ISSUES IN ROUTING PROTOCOLS

The source node broadcasts a route request to discover a route to the destination node. When an intermediate node receives the route request, it appends its identifier in the request packet and relays the request. The destination node receives the route request, a route has been set up and carried in the route request. The destination node generates a route reply containing the route and sends it back to the source node along the reverse of the routing. The contemporary routing protocols for ad-hoc networks with dynamically changing topology are not designed to accommodate defense against malicious attackers. Today's routing algorithm are not able to common security threats. Most of the existing ad hoc routing protocols do not accommodate any security highly vulnerable to attacks. Threats and attacks against ad hoc routing under several areas of application and suggested [3] Routing information signed by each node will not work compromised nodes can generate valid signatures using their private keys. Detection of compromised nodes through routing information is difficult due to the dynamic topology of ad hoc network in protocol, the nodes in an ad hoc network different security attributes are classified into different trust levels. The trust level can be decided by an internal hierarchy of privileges in an organization. The nodes of the same trust level share a secret key. When a source constructs a route discovery message, specifies the required security level for the route. The route discovery message can be encrypted by using the secret key shared by nodes of same trust level. Only the intermediate nodes that required security level can process the message only these nodes can decrypt the message. Other nodes drop it. This protocol provides some protection to routing messages.

The remaining problems are: Is the trust level fixed or can be changed? How to distribute key within the same trust level? Haas [4] proposed a secure routing protocol (SRP) for ad hoc networks. The assumption of SRP is the existence of a Security Association between a source node and a destination node, through which the source node and the destinte. The most important secure measure used in SRP is Message Authentication Code, which is calculated by using the shared secret key two ends.

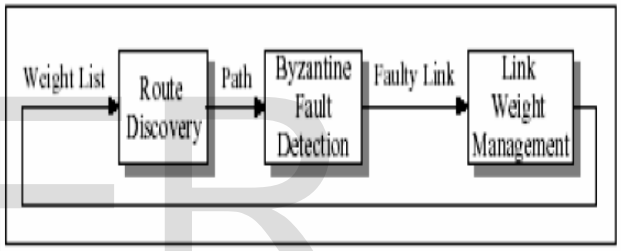

Fig.2 Phases of Byzantine algorithm

The above fig depicts the 3 phases of the Byzantine algorithm, i.e. Link Weight Management, Route Discovery with Fault Avoidance, and Byzantine Fault Detection.

4. PREVENTION USING SYMMETRIC CRYPTOGRAPHY: SECURITY-AWARE AD HOC ROUTING (SAR)

SAR is an attempt to use traditional shared symmetric key encryption in order to provide a higher level of security in ad hoc networks. SAR can basically extend any of the current ad hoc routing protocols without any major issues. The SAR protocol makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Although current routing protocols discover the shortest path between two nodes, The different trust levels are implemented using shared symmetric keys. In order for a node to forward or receive a packet it first has to decrypt it and therefore it needs the required key. Any nodes not on the requested trust level will not have the key and cannot forward or read the packets. Every node sending a packet decides what trust level to use for the transfer and thereby decides the trust level required by

every node that will forward the packet to its final destination.

Nothing is done to prevent intervention of a possibly malicious node from being used for routing, as long as they have the required key.

If a malicious node somehow retrieves the required key the protocol has no further security measure to prevent against the attacker from bringing the entire network to a standstill.

There is excessive encryption and decryption required at each hop. Since we are dealing with mobile environments the extra.

Detection and Reaction: Confident[11]

Trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes. The protocol has been described using Dynamic Source Routing (DSR) in the network layer.

Each node consists of 4 basic components:

1. *The Monitor:* watches its neighbors for any malicious behavior. If such behavior is detected, the reputation system is invoked.

2. *The Reputation System:* manages a table consisting of entries for each node and its ratings. Ratings are changed according to a rate function that assigns different weights to the type of behavior detected.

3. *The Trust Manager:* responsible for calculating trust levels of nodes and dealing with all incoming and outgoing alarm messages.

4. *The Path Manager:* manages all path information, i.e. adds, deletes or updates paths according to the feedback it receives from the reputation system.

5. PREVENTION USING ONE-WAY HASH CHAINS: SEAD

The main objective of the protocol is to avoid any malicious node from falsely advertising a better route or tamper the sequence number in the packet that it received from the source. They basically implement features to protect modification of routing information such as metric, sequence number and source route. SEAD uses a one-way hash chains for authenticating the metric and the sequence number.

Each node creates a one-way hash chain and uses the elements in groups of 'm' (given m as the diameter of the network) for each sequence number. Each node uses a specific single next element from its hash chain in each routing update that it sends about itself (metric 0). The upper bound of the network is denoted by (m-1). An entry is authenticated by using the sequence number in that entry to determine a contiguous group of m elements from that destination node's hash chain, one element of which must be used to authenticate that routing update. The one-way nature of hash chains prevents any node from advertising a route with a greater sequence number than the source's sequence number.

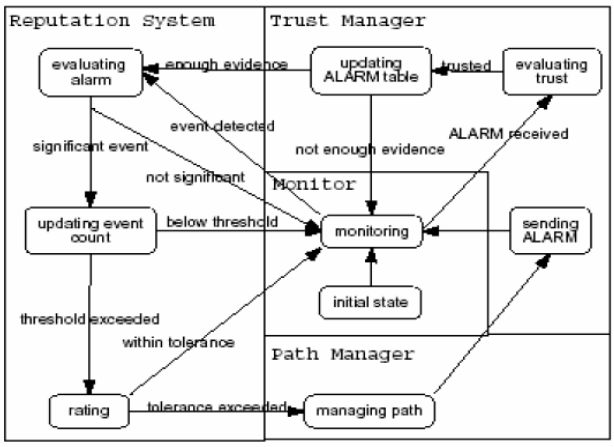

Fig.3 Trust architecture and FMS within each node of a Confidant

6. CONCLUSION AND FUTURE WORKS

Securing an ad hoc network is not a simple task. First of all, algorithm that secures the network must ensure the authentication procedure. In other words, ensure the process that aim to confirm that a committing is the node that he claims to be previous work shows that with less transmission in VANET. P-coding a light-weight encryption scheme can be used with network coding, to reduce the energy consumption as well as security in VANET. P-coding is efficient in computation and requires minimum energy for encryption decryption operaction. The identity of each committing is confirmed based on four traditional factors of authentication, which can be used to confirm the identity of a committing:

- Use Information that only the committing knows.
- Use Information that only the committing features.
- Use Information that characterizes the committing in a given context.
- Use Information that only the committing may occur.

Other authentication factors can sometimes be used as time constraints or location capabilities. But it cannot guarantee non-repudiation of message.

7. REFERENCES

[1] R. Hekmat, Ad hoc Networks : Fundamental Properties and Network Topologies, The Netherlands.: Springer, 2006.

[2] J.-Z. Sun, «Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing,» Finland.

[3] Levente Buttyan and jean-pierre Hubaux Enforcing Service Availability in mobile Ad-hoc WANs proceedings of the IEEE/ACM workshop on mobile Ad Hoc networking and computing(mobiHoc),Boston,MA,USA,August 2000.

[4] Sonja Buchegger and Jean-Yves Le Boudec. Cooperative Routing in mobile Ad-hoc Networks: current efforts jAgainst Malice and selfishness in lecture Notes on Informatics, mobile internet workshop, Informatik 2002, Dortmund, GJermany, OFctober 2002. Springer.

[5] S.Singeh, CJ.Raghavendra, and J.Stepanek, "power-Aware Broadcasting in mobile Ad Hoc Networks, in proce. IEEE PIMRC, 1999, pp. 1-10.

[6] J.Wieselthier, G.Nguyen, and A.Ephremides, "Algorithms for energy-efficient multicasting in static Ad Hoc wireless Networks, "mobile network.

[7] J.P. Vilela, L.Lima, and J.Barros, "Lightweight security for Network Coding, "in proc. IEEE ICCC, may 2008,pp.1750-1754.

[8] N.R. potlapally, S.Ravi, A.Raghunathan, and N.K. Jha, "A study of the energy consumption characteristics of cryptographic Algorithm and security protocols, "IEEE trans. Mobile computing, vol. 5, no.2,pp. 128-143,feb.2006.

[9] pietro michiardi, Refik molva core: A collaborative Reputation mechanism to enforce node cooperation in mobile Ad Hoc networks in communication and multimedia security 2002 conference.

[10] Sonja Buchegger and jen-Yves le Boudec. Performance Analysis of the CONFIDENT protocol: cooperation of Nodes-Fairness in Distributed Ad-Hoc networks in proceedings of IEEE/ACM workshop on mobile Ad Hoc networking and computing (mobiHoc),Lausanne, CH, June 20092.IEEE.

[11] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.