Journal of Biodiversity and Environmental Sciences (JBES)
ISSN: 2220-6663 (Print) 2222-3045 (Online)
Vol. 6, No. 6, p. 589-595, 2015
http://www.innspub.net

INNSPUB

RESEARCH PAPER

OPEN ACCESS

Investigating and comparing safe routers in adhoc networks

Somayyeh Haghtalabi*, Mehdi Golshan, Mostafa Jahangir, Reza Saboor

Department of Computer Engineering, Islamic Azad University, sepidan Branch, Sepidan, Iran

Article published on June 30, 2015

Key words: Adhoc networks, Safety, Safe, Rout finding.

Abstract

Adhoc networks are networks are nodes non-structurally related nodes with no consistent resource for organizing them. One of the most difficult problems in Ad-Hoc networks is rout finding. Since the nodes are displaced in Ad-Hoc networks, they get distant from adjacent boards and hence, the network topology changes all the time. Safety in Ad-hoc networks especially for military ones is very vital. As nodes don't have constant position, any invading node can penetrate the network easily and gets the safety of information or rout finding of all or a part of the network disordered; especially giving the fact that most of the rout finding methods in the network tend to believe in all nodes. This survey investigates the pros and cons of three protocols of safe rout finding and we survey some of the main algorithms in this significant like SEAD and ARANA algorithms.

***Corresponding Author:** Somayyeh Haghtalabi ✉ s.haghtalabi@gmail.com

Introduction

Unstability among adhoc networks can cause the rout changing of both groups. This is the fact that separates these networks form other wireless networks. In spite of these problems, the adhoc networks are used in different cases. The reason is speed and easiness of performing these networks and their independence from other pre-structured forms. The nodes of the networks are responsible for finding the rout by themselves. There is not only a way to find the routs.

That is, there is no network assisting rout such as switches or routers and the finding the rout is done by the network forming nodes, themselves (David, 2002). End- to-end structure causes each node to serve both as a host and router and considering that the nodes are being displaced all the time, one can conclude that there is no distinct between inside and outside of the network. As mentioned before, lack of reliable infrastructures is regarded as an important factor in having the issue of safety more complicated in Ad-Hoc networks. In order to solve this problem, it is not possible to appoint a node as the source of decision-making because the one of the aims of Ad-Hoc networks is not to be confined to a specific node. In a case that such node as the source of network safety is invaded by the outside of the network, the safety functionality of the whole network is endangered.

One of the reasons causing the Ad-hoc networks more vulnerable to different kinds of invades is the confinement of these sorts of networks regarding electronic and processing capacity.

Because the nodes of these networks are mostly formed by tiny portable machines such as PDAs; therefore, performing methods requiring high processing capacity (e.g. general key encrypting) is not feasible. Since wireless sending and receiving needs wasting a lot of electronic strength, if a node is located in a loop, sending unnecessary packages, in a short time it loses its communication with the network due to running out of energy. The aim of this paper is investigating and comparing safe routers in adhoc networks.

Material and methods

Safety in Ad-Hoc networks

The abundant using of Ad-Hoc networks in military environments and other stings sensitive safety requires safety as a basic necessity form the merging of these networks. Besides this necessity, providing safety in these networks has its own troubles. Specific structure of wireless Ad-Hoc has caused novel problems for safety of these networks (Mitchell, 2002; Stallings, 2002). The problem of performing safety in Ad-Hoc networks tends to be originated from some main factors:

Wireless transmitting setting

Using a wireless setting can make the system sensitive to a mass range of invasions that these invasions can range from a simple listening to fabricating the identity by another node.

Dynamic typology

In general, the attendance of nodes in the network is a kind of dynamic. That is, they get enrolled and separated from the networks all the time and therefore, no one should count on a consistent link in terms of safety. Diminishing of a link can also be due to one-way status of the wireless link (Yih-Chun, 2003).

Lack of an infrastructure to consider as determining factor in the networks.

This feature in Ad-Hoc networks has caused not to be any concentrated access control and the nodes are evaluated regarding originality.

The weakness related to the network

In addition to the specific features of the network that makes the structure sensitive to safety invades, some weaknesses are due to low capability of nodes processing.

End- to-end structure causes each node to serve both as a host and router and considering that the nodes are being displaced all the time, one can conclude that there is no distinct between inside and outside of the network. As mentioned before, lack of reliable infrastructures is regarded as an important factor in having the issue of safety more complicated in Ad-Hoc networks.

In order to solve this problem, it is not possible to appoint a node as the source of decision-making because the one of the aims of Ad-Hoc networks is not to be confined to a specific node. In a case that such node as the source of network safety is invaded by the outside of the network, the safety functionality of the whole network is endangered.

One of the reasons causing the Ad-hoc networks more vulnerable to different kinds of invades is the confinement of these sorts of networks regarding electronic and processing capacity. Because the nodes of these networks are mostly formed by tiny portable machines such as PDAs; therefore, performing methods requiring high processing capacity (e.g. general key encrypting) is not feasible. Since wireless sending and receiving needs wasting a lot of electronic strength, if a node is located in a loop, sending unnecessary packages, in a short time it loses its communication with the network due to running out of energy.

Result and discussion

Safe rout-finding algorithms in Ad-Hoc networks

Safe rout finding in Ad-Hoc networks is a defined term indicates those kinds of rout finding elaborating on encrypting methods to provide the network with safety. This act can take place using the processes of originality or non-deniability in rout finding. The methods of making safety in rout finding can be different based on the tool used and their usage method as well. The methods used for safe rout finding is not limited but the similarity between them are a lot (Oppermann *et al.,* 2004).

SEAD rout finding algorithm

Rout findings based on Distance Vector constitute variety of table rout finding subscales. These sorts of algorithms have a simple structure and can be performed easily. The functionality of them is fast and they need to a low strength of processing. These kinds of methods are used massively in wired networks and internet (Yih-Chun *et al.*, 2002).Therefore, they are counted as first options to be used for rout finding by the emerging of the Ad-Hoc networks (Mpitziopoulos *et al.*, 2009). But as mentioned before, due to changing situation of the network, they have less powerful functionality in comparison to situational routers (Wood *et al.*, 2007).

DSDV and its optimized module, DSDV-SQ are one of the first and simultaneously the effective algorithms of rout finding based on Distance Vector suggested for AD-Hoc networks. This algorithm is suggested for safe situations and based on nodes complete coordination and is vulnerable facing the invasions mentioned in previous chapter.

The structure of DSDV rout finding is based on a table of rout finding in each node. The information provided in each line of the table is related to each one of the network nodes. The information includes the distance till the aimed node (based on the numbers of jumps), serial number and next jump (on a route between the node until the next target node) (Stutzman, 1997; Hsiao *et al.,* 2011). Each node sends its rout finding table to adjacent nodes according to a specific time. The adjacent nodes also elaborate on amending their rout finding tables according to thisnew receiving information. In order to prevent old updates in rout finding process, the serial number is used. Another usage of serial number is avoiding loop formation in rout finding process. Therefore, there are two sections of information in processes mentioned above, determining decision-making in rout finding:

- Serial number
- Metric or distance (based on jump numbers)

The main purpose of designing SEAD (Yih-Chun *et al.*, 2002) founded based on DSDV-SQ is also to prepare the possibility of measuring the originality for these two sections of rout finding information. In general, there are two main modules of gauging originality in SEAD. The first one as mentioned before is the metric and serial number originality and another one is the originality of the adjacent nodes. While DSDV is sensitive to all invasions taking place to the structure of rout finding, SEAD is resistant against all the aforementioned invasions(this does not mean the safety of whole protocol but other methods can be affected). The main purpose of SEAD designers is to make possible gauging of the originality for all displaced information of routing. The first solution which is often suggested is asymmetric encryption but there three problems with this solution:

1. The evading node can busy the affected node's processing power via sending lots of fabricated updates. Performing this act, a DOS invasion is attempted in layers of the network. As mentioned before, asymmetric encryption requires a high volume of math calculations.
2. If a node of network gets captured by the enemy, it can make chaos in adjacent rout finding nodes by sending a table consisting of all metrics.
3. Even if there is no evading node, asymmetric encryption causes loss of lots of resources during the process of sending messages of rout finding due to overwhelming.

For avoiding the above-mentioned problems in SEAD, "hash series" is used for gauging the originality performed before in wired networks (Sung *et al.*, 2004). In spite of this, SEAD is the first module of using this method in AD-Hoc networks.

ARAN rout finding algorithm

ARAN rout finding (Stutzman, 1997) is also a situational method that the essence of its functionality is based on AODV. At first, the author divides the settings for using Ad-Hoc networks into three subfields. The first subfield is ones where in rout finding algorithms are characterized based on the following conditions:

- Rout finding signaling should not be fabricated. The evading node outside of the network should not be able to send false messages into the network.
- Rout finding messages ought not to be changed but according to the rules of rout finding.
- The evading node is not allowed to make loop in rout finding.
- The evading node should not be able to impose a short fabricated route to the network.

For the managed open conditions, another condition is added to the above conditions:

- The chosen rout should not pass through the node that is not approved regarding originality. Here, the author does not classify the situation when two members of network invade the network, domestically.

The third setting regards evading ones where besides the abovementioned conditions, one coming beneath also should be taken for granted:

- The network topology ought not to be obvious for neither evading (invading) nodes nor the network nodes.

ARAN structure

For designing ARAN protocol, the setting condition is regarded as open or managed open. Therefore, there is the possibility of inspecting and analyzing traffic nodes of the network for the invader. The first hypothesis is that there is a reliable resource in network (Wood *et al.*, 2003). This resource can be a node or a series of them. The responsibility of this node is to assign Certificate Authority (CA) for network nodes. The second hypothesis is that all of the nodes know the general key (CA). In order to enter the network, each node should receive a certificate from CA. This certificate is for node A is as the following main form:

$$T \to A: Cert_A = [IP_A, K_{A+}, t, e]K_{T-}$$

In this certificate, IP_A address is the IP node for A and K_{A+} is the general key for this node and "t" and "e" are the times of offspring and expiry of this node, respectively. Whole of the certificate is also encrypted by personal key (CA) of K_{T-}.

After receiving the certificate, if the node A tends to make a rout to node x, it makes a package of requesting for rout as the following and sends it to its adjacent:

$$A \to *: [RREQ, IP_X, N_A]K_{A-}, Cert_A.$$

In above passage, N_A is number counted as a serial number for package of requesting for rout. The whole package is encrypted by the personal key of A. therefore; its content is reachable through network members. The middle node receiving this package also must be investigated via general key of CA regarding the authority of node (Liu *et al.*, 2008). This is in a case the certificate is valid; the node originality is endorsed on the rout using the general key of "A". After reaching the package content, IP_A and N_A are investigated to know whether or not the package has been received before. In a case the package is not received up to know, its content is endorsed again by the specific key and after being located next to the certificate, it is sent. Therefore, the package sent by "B" will be as follow:

$$B \to *: [[RREQ, IP_X, N_A]K_{A-}]K_{B-}, Cert_A, Cert_B.$$

Let's consider this assumption that package sent by "B" is sent by "C". After that the authentication and originality of "A" and "B" nodes certificates, the endorsements of these two nodes are investigated in receiving packages. After this, the endorsement and certificate of the node "B" is taken away and replaced by "C" ones on the package:

$$C \to *: [[RREQ, IP_X, N_A]K_{A-}]K_{c-}, Cert_A, Cert_c$$

Now, if the packaged with the mentioned definitions is reached by node "X", the inspection of originality also takes place by this node and in a case that the authentication is approved, it makes a package of requesting to the rout as follow and sends is to the node to which the package is received from (i.e. D):

$$X \to D: [RREP, IP_A, N_A]K_{X-}, Cert_X$$

The node of "D" also inspects the authentication of both certificate and endorsement of node "X" and considering the fact that it has recorded in its memory from which node it has received the package request for rout, it sends the response to the request as well as the both endorsement and certificate by itself to this node:

$$D \to C: [[RREP, IP_A, N_A]K_{X-}]K_{D-}, Cert_X, Cert_D$$

After approval of the authentication of the "X" and "D" endorsements, "D" endorsement is taken away and replaced by "C" on the package and the package is sent to the node from where in the package has been requested (Madhyastha *et al.*, 2009).

Presenting above structure prevents neither authenticated nor received certificate nodes from CA pass through the chosen rout. This method causes the insurance of the network inevitably and if a node attempts to affect the functionality of the network via repetitive sending of non-authenticated packages, it could be traced easily. Although the content of the packages sent to whole nodes throughout the rout is evident, none of the nodes can modify the content because they should fabricate the departing node endorsement on the package if they try to make change that this is not possible. In spite of the positive points talked about the algorithm, there are some safety shortcomings with it.

ARAN safety shortcomings

- The structure of the defined method is based on asymmetric encryption as well as electronic endorsement that this problem remains the network potentially vulnerable DOS invasions (Hsiao *et al.*, 2011). especially due this fact that in each jumping of

the middle nodes, the asymmetric encryption ought to be used four times to decode the encryptions and inspection of the endorsement authentication for receiving packages and then this encryption should be used again to endorse packages. Performing asymmetric encryption is also difficult and time-consuming for the fastest routers in the wired networks and knowing that nodes of the Ad-Hoc networks are formed by tools with finite electrical and processing strength, the suggested method is not optimized at all in terms of processing.

- The suggested method has nothing to point about the way of endowing specific key to the nodes and the receiving certificate form CA only includes the general key for the target node.

- The presented structure depended on CA is active. If CA functionality is affected by any means, other nodes of the network are not able to communicate each other.

- The network is severely sensitive to the Wormhole evading. A package of requesting rout can be delivered to the target node fast through a specific link of evading nodes. Using asymmetric encryption for four times reduces the jumping of the suggested method in such a way that for making the target invasion it is not necessary for the invader to have a high speed link.

- Because of using time parameter as the determining factor, the network is completely vulnerable against rushing invasions. The evading node can send the receiving package without processing and since other nodes of the side ought to consume along time on existing endorsements processing, the evading node locates in a proper situation to invade.

Conclusion

This survey has investigated the pros and cons of rout finding algorithm safety in adhoc networks possessing a significant role in algorithm election. One of the future works is to compare more algorithms.

References

Chan H, Perrig A, Song D. 2003. Random Key Predistribution Schemes for Sensor Networks. In Proceedings of the IEEE Symposium on Security and Privacy.

Charles E, Perkins Elizabeth M, Belding-Royer, Samir R. 2003. Ad Hoc On Demand Distance Vector (AODV) Routing. Internet-Draft, draft-ietf-manetaodv-10 txt.

David B, Johnson David A, Maltz Yih-Chun Hu, Jorjeta G, Jetcheva. 2002. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). Internet-Draft, draft-ietf-manet-dsr- 07.

Du W, Deng J, Han S, Varshney PK. 2003. Establishing Pairwise Keys in Distributed Sensor Networks. In Proceedings of the ACM Conference on Computer and Communications Security.

Hsiao HC, Studer A, Chen C, Perrig A, Bai F, Bellur B, Iyer A. 2011. Flooding-Resilient Broadcast Authentication for VANETs. In Proc of Mobi Com.

Jia L, Basescu C, Kim THJ, Perrig A, Hu YC, Zhang F. 2014. Mechanized network origin and path authenticity proofs. Technical Report CMU-CyLab-14-007. Carnegie Mellon University.

Kang MS, Lee SB, Gligor VD. 2013. The CrossfireAttack. In Proc of IEEE Security and Privacy.

LiJ, Sung M, Xu J, Li L. 2004. Large-Scale IP TracebackinHigh-Speed Internet: Practical Techniques and Theoretical Foundation. In Proc. of IEEE Security and Privacy.

Liu B, Chiang JT, Haas JJ, Hu YC. 2010. CowardAttacks in Vehicular Networks. Mobile Computing and Communications Review.

Liu X, Li A, Yang X, Wetherall D. 2008. Passport: Secureand Adoptable Source Authentication. In Proc.

Madhyastha HV, Katz-Bassett E, Anderson T, Krishnamurthy A, Venkataramani A. 2009. iPlane Nano: Path Prediction for Peer-to-peer Applications. In Proc.

Mitchell J. 2002. Security for Mobility. IEE Press January.

Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G. 2009. JAID: analgorithm for data fusion and jamming avoidance on distributed sensornetworks, Pervasive Mobile Comput **5 (2),** 135–147.

Oppermann I, Stoica L, Rabbachin A, Shelby Z, Haapola J. 2004. UWB wirelesssensor networks: UWEN-a practical example, IEEE Commun. Mag **42 (12)**.

Stallings W. 2002. Cryptography & Network Security, Prentice Hall.

Stutzman WL, Thiele GA. 1997. Antenna Theory and Design, second ed., J. Wiley, New York.

Wood AD, Stankovic JA, Son SH. 2003. a jammed-area mapping service for sensor networks, in: Proceedings of the 24th IEEE International Real-Time Systems Symposium, RTSS 03, IEEE Computer Society. Washington. DC, USA p. 286.

Wood AD, Stankovic JA, Zhou G. 2007. DEEJAM: defeating energy-efficientjamming in IEEE 802.15.4-based wireless networks, in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad-Hoc Communications and Networks 60–69.

Xu W, Trappe W, Zhang Y, Wood T. 2005. The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad-Hoc Networking and Computing – Mobi Hoc 05.

Yih-Chun Hu, Adrian Perrig R, David B, Johnson A. 2002. A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (Mobi Com 2002), pages 12–23.

Yih-Chun Hu, David B, Adrian Perrig J. 2002. Secure Effcient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02) **3**.13.

Yih-Chun Hu. 2003. Enabling Secure High-Performance Wireless Ad Hoc Networking. PHD thesis, School of Computer Science Computer Science Department Carnegie Mellon University (CMU-CS-03-144).