Journal of Advanced Computer Science & Technology, 4 (1) (2015) 116-121
www.sciencepubco.com/index.php/JACST
©Science Publishing Corporation
doi: 10.14419/jacst.v4i1.4156
Research Paper

Strategies for enhancing the accuracy and security in ad hoc networks

Behnam Rahmani Delijani [1]*, Hassan Tavakoli [2]

[1] *MSc Student, University of Guilan , University Campus 2, Rasht Branch , Iran*
[2] *Assistant Professor in Department of Electrical Engineering, Faculty of Technology & Engineering, University of Guilan, Rasht Branch, Iran*
**Corresponding author E-mail: rahmani69@msc.guilan.ac.ir*

Abstract

Ad Hoc networks are a type of mobile wireless networks composed of mobile and stationary nodes which are moving freely and independently or they are stable. Setting up Ad Hoc networks is very simple and as these networks do not need a standard fixed infrastructure and central legal license, their setting up cost is very low. So, in specials, temporary or short-term situations such as flood, earthquake and fire as well as in military environments where all telecommunication platforms are destroyed, these networks are used as a new solution for creating communications between network elements. As Ad Hoc networks have a limited energy and nodes are continuously displacing, consequently, the accuracy of these networks is important. Nodes can be easily added to the network at any time or leave the network. It not only leads to easy creation of a network and its fast, easy and low-cost expansion, but also makes it possible for an enemy to enter the network. Therefore, the security of these networks must also be considered. In this paper, using a new method and imposing limitations on some network nodes, we created a more reliable network with higher accuracy and security.

Keywords: *Ad Hoc Networks; Accuracy; Security; Forwarding A Virtual Package; Backbone.*

1. Introduction

Ad Hoc networks were created for military reasons more than 70 years ago. The first Ad Hoc network was created by DARPA [1]. At that time, this network was called “packet radio” [2]. An example of Ad Hoc networks is battle fighters’ networks and their mobile bases in the battle field. It was later determined that these networks can also be useful in commercial and industrial sectors [3]. First, we review the meaning of Ad Hoc term. Ad Hoc means “only purpose for this”. This term is usually used where the solution of a special problem or taking a special responsibility is considered. The Ad Hoc network is also called Mesh Network. Because all networks in the area under the coverage of the Ad Hoc network are aware of each other’s existence and can communicate with each other [4], [5]. It is like implementing a physical network based on the mesh topology. Each of Ad Hoc network’s nodes is equipped with a wireless transmitter and receiver system and in addition, each node may be the host computer or intermediate routing node [6]. Nodes will cooperate with each other and communicate through the package exchange [7]. Nodes in the network do not have a central and centralized management and are responsible for the creation, operation and maintenance of the network by themselves [8]. One of the characteristics of these networks is the high efficiency, low bandwidth, low energy consumption and lack of any central base [9]. Ad Hoc networks are usually small networks, unless one or more nodes connect to other networks and share their data and information with other nodes. In this case, by connecting to other networks with different structures, wireless Ad Hoc networks create larger networks [10]. The rest of the paper is organized as follows:

In section 2, we will propose a concept called forwarding a virtual package by which the relative accuracy and security of some new nodes can be evaluated with no problem. In section 3, the network’s backbone will be studied. In section 4, we will study different types of packages which are received by the destination node. Section 5 explains the strategy for imposing limitations in order to increase the accuracy and security of Ad Hoc networks. Finally, in section 6, the conclusion is provided.

2. Forwarding a virtual package

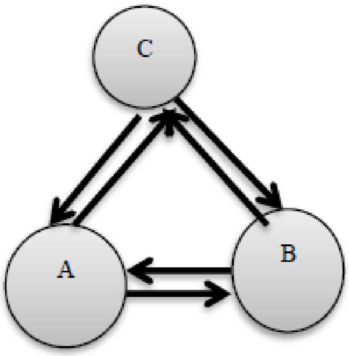


Fig. 1: Forwarding a Virtual Package

In an Ad Hoc network, all nodes are not reliable and we have nodes with different reliability rates in the network. In some case, by forwarding a virtual package, we can check the security of one or more nodes and consequently, increase or decrease the score of that node. According to figure 1, nodes A and B are secure and node C is unsecure. A secure node is a node which is not an enemy or this possibility is very low. According to the duration of the node’s activity in the network and by observing the history of node’s activity, we obtain this possibility. However, our certainty of secure nodes is not an absolute certainty and is relative. In contrast, an unsecure node is a node which recently entered the network and there is not much history of its activity in the network. As it is obvious in figure 1, all nodes have a mutual relationship. In this case, node A which wants to forward a message to node B, once must forward it through a direct direction and once again through intermediate node C. In addition, node A directly informs node B that this message will be forward through node C once again. If node C is a healthy node and receives the message correctly, nodes A and B will trust node C more. But if node C is not healthy and or is an enemy, and change the message optionally or if it is a selfish node which prevents from routing in order to save its energy, node C will lose the trust of nodes A and B. By this simple operation, the security of node C is evaluated. For the virtual forwarding and checking the security of one or more nodes, it is clear that messages are used which are not confidential and are only some normal messages; so, if unknown new nodes are enemies, no serious damage is imposed on the network. Meantime, the direct relationship between nodes A and b must be hidden from node C tested here.

3. Backbone

In a wireless Ad Hoc network, we consider one or more nodes which have special conditions and communications as backbone nodes. Conditions and characteristics of backbone nodes are as follows:

3.1. The number of backbone nodes

Nodes which are considered as backbone nodes in a wireless Ad hoc network can be variable from one to several nodes based on different cases and situations in the network. Usually, for the proper coverage of backbone in the entire network, several nodes are used. Some of these conditions include: the network’s security rate, total number of network’s nodes, accuracy and quality of data forwarded in the network, number of input and output nodes, etc.

3.2. Reliability of backbone nodes

The backbone must be selected from network’s reliable nodes and in fact, it is better to select nodes which are present in the network for a longer duration and have a good record. In the backbone, new nodes with limited backgrounds must not be used. Reliable nodes are nodes which are reliable in two general dimensions of security and accuracy. These two dimensions are explained in the following section:

3.2.1. Security

As backbone nodes are usually present in the network from the beginning to the end of communications, these nodes must not be enemy nodes. Otherwise, security of the entire network is endangered and irreversible damages are imposed

on the network. In this case, nodes in which $P < 0.9$, i.e. enemy nodes with 90% possibility, cannot be a member of the backbone group.
P = the possibility that nodes are not enemy
If $P \geq 0.9$, nodes can be members of the backbone.
If $P < 0.9$, nodes cannot be members of the backbone.

3.2.2. Accuracy

Backbone nodes must be reliable from accuracy point of view, i.e. their energy (battery) must be enough for different activities in the network (such as routing, package transfer, route detection, maintaining routes' history, etc.). It is better that backbone nodes be the last nodes that lose their energy. In addition, for the network's survival, it is better that these nodes be the last ones leaving the network for any reason.

In some cases where our Ad Hoc network is a network with a long life, i.e. the network is used in the long term so that the network's lifetime is several times the life of each node, for surviving the network's backbone which consequently leads to the survival of the network itself, it is necessary to estimate the approximate lifetime of each of backbone nodes for their correct services in the network. Then, before leaving the network or in some similar cases, this situation must be notified to the network and leave the network by selecting a suitable alternative. Given that B is the battery (energy) amount of each node, we have:
B = the battery (energy) amount of each node
$0\% \leq B \leq 100\%$
If $B > 15\%$, it can be a member of the backbone and can have activities.
If $5\% \leq B \leq 15\%$, it can be a member of the backbone and perform alternative operations.
If $B < 5\%$, it cannot be a member of the backbone.

3.3. Backbone nodes connections

If we have several nodes as backbone nodes, for the guarantee of network's security and accuracy by our network backbone, its nodes must have a continuous connection. Their minimum connection must be a chain and single input - single output connection. Figure 2 shows this case:

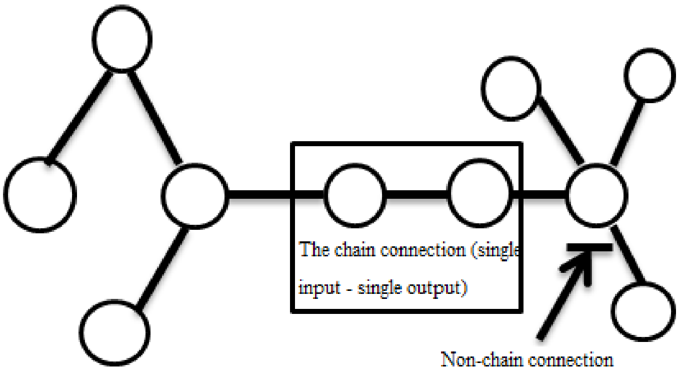


Fig. 2: Presentation of Chain and Non-Chain Connections in the Backbone

If some nodes want to form the backbone of a network, they must have some common parts of the aforementioned cases as figure 3:

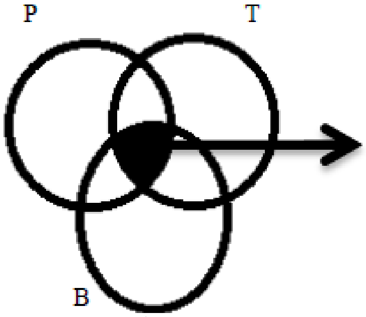
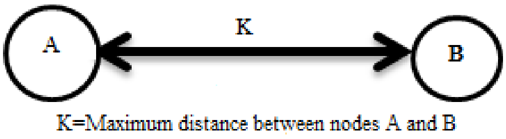


Fig. 3: Requirements for Membership in the Backbone

Nodes which can be a member of the backbone
P = the possibility that nodes are not enemy
B = the battery (energy) amount of each node
T = the history and presence of each node with a good background (activity time)

3.4. Adjusting the appropriate distance between nodes for the survival of the backbone

For the high survivability of our Ad Hoc network and its high reliability coefficient from accuracy and security points of view, the network's backbone must not be destroyed. Backbone nodes are not necessarily stationary nodes. In addition, they not only may maintain the network, but also may cooperate and help in network's different operations, including routing. Therefore, for the minimum connection of nodes (when two backbone nodes are connected in the form of a chain and single input - single output), nodes must be placed in a suitable distance. The suitable minimum and maximum distance of two backbone nodes from each other depends on the network's security, the energy amount of nodes, signal coverage of wireless devices, etc. Figure 4 shows this distance.



MAX (A, B) = K (m)

Fig. 4: Suitable Distance between Backbone Nodes

If the distance between nodes A and B is more than the signal coverage, two nodes must get close to each other in order to prevent from the backbone's breakdown. Furthermore, the nodes' distance from each other must not be so close. In this case, whether the distance between two nodes will be so long or a node in the backbone will be insignificant and can be removed.

3.5. Different types of messages received by the destination node

In Ad Hoc networks, packages forwarded by the transmitter have three general states:
A) Packages which are forwarded by the transmitter and correctly received by the receiver. In fact, in this state, the package received by the destination receiver is exactly the package forwarded by the transmitter. When a package is forwarded and received in this form, source and destination nodes will trust intermediate nodes which routed this package more and try to use more reliable routes in their next forwards until they exist.
B) Packages forwarded by the transmitter, but not received by the receiver. In this state, for removing the problem, the transmitter will forward the package through other routes. But, if there is not another route, the transmitter will forward the package through that existing single route again. If the package is not forwarded, the binary search tries to find the problem among intermediate nodes in the source and destination.

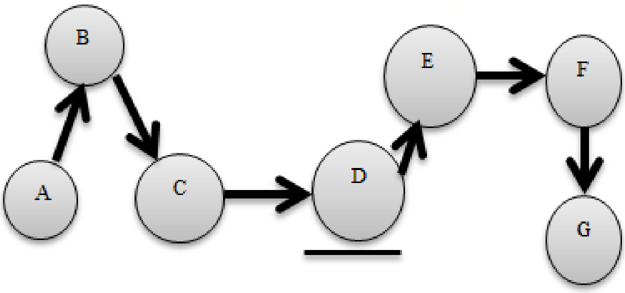


Fig. 5: Presentation of Finding the Problematic Node by the Binary Search

In this state, according to figure 5, instead of considering node G as the destination, the transmitter and source A which are trying to forward the message to destination G will select the intermediate node between A and G as the destination by the binary search. In this case, our new destination is D. If message A is correctly received by C, we will find out that there is a problem in the second half of the route, i.e. between nodes D to G, but if the message is not correctly received by node D, for solving the problem, we will continue the binary searching and finding the intermediate node in the center until we find the problematic node. After finding the problematic node, we will try to solve the problem by forwarding another node to that point or using other methods.
C) Packages forwarded by the transmitter, but the receiver will receive another amount of packages which is not equivalent to the transmitter's amount. In general, the incorrect forwarding of packages can be due to the

telecommunication error probability, the accuracy or the presence of an enemy node along the way. We use two methods for reviewing this state:

The first method: From packages with different amounts in the transmitter and receiver, we will randomly open one or more packages and match the transmitter and receiver bits: If their difference is not more than one or two bits, we can blame the accuracy, distance and the possible error in links with a high probability, but if their difference is much more, it can be due to the presence of an enemy intermediate node in the network and along the route between the source and destination. It is worth noting that in each network, we will review several packages in order to match the amount received by the receiver with the amount forwarded by the transmitter, and also, the issue that how much error bit is negligible depends on the security and significance of packages' destiny in the network and the number of packages forwarded correctly or incorrectly, etc. Figure 6 shows the aforementioned cases.

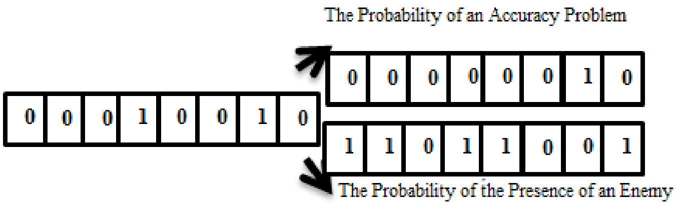

The Probability of an Accuracy Problem
0 0 0 0 0 0 1 0
0 0 0 1 0 0 1 0
1 1 0 1 1 0 0 1
The Probability of the Presence of an Enemy

Fig. 6: The Comparison between Forwarded and Received Bits

The second method: The packages which their messages were arrived at the destination but are incorrect will be calculated according to the ratio of signal power received by the receiver to the signal power forwarded by the transmitter and through formula (1):

$$\alpha = \frac{P_t}{P_r} = \frac{(4\prod d)^2}{\lambda^2} = \frac{(4\prod f d)^2}{c^2} \qquad (1)$$

$\alpha \geq 1$

α : The ratio of the signal power of transmitter to the signal power of the receiver

Pt : Signal power in the transmitter's antenna

Pr : Signal power in the receiver's antenna

λ : Signal wavelength

F: Signal frequency

D: Propagation distance between antennas (meter)

C: Speed of light

The value of α is larger than 1. If the value of α is close to 1, the distance between intermediate nodes is low and they have a suitable accuracy, and the enemy node must be found. But, if the value of α is larger than 1, not only there is the possibility of the enemy presence, but also there is the possibility of a telecommunication error in links. Figure 7 shows this situation.

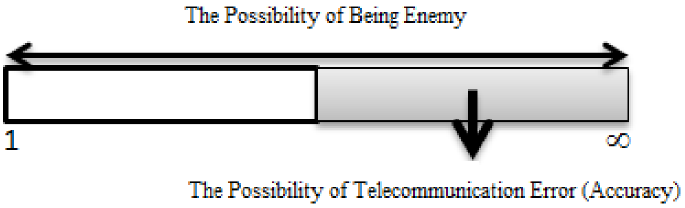

The Possibility of Being Enemy
1
∞
The Possibility of Telecommunication Error (Accuracy)

Fig. 7: The Possibility of Accuracy and Being Enemy

Figure 8 shows that with the increase of α value, the information accuracy is reduced.

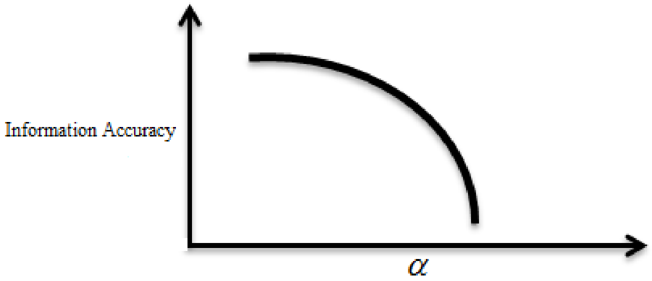


Fig. 8: The Information Accuracy_α Schema

It is obvious that in Ad Hoc networks, for reviewing and identifying the amount of accuracy and security, it is better to use the Hybrid method and a combination both methods in order to obtain the best result.

4. Imposing limitations for enhancing the network's accuracy and security

An Ad Hoc network is composed of a number of secure, insecure and semi-secure nodes. In previous sections, according to the value of α , we found out that distance is an important factor in the accuracy. In order that routings and exchange of messages are done through more reliable nodes, we impose limitations. Before discussing these limitations, we get familiar with the concept of relay:

Relay: Relay is in fact the method of forwarding information which is divided into two types:

Amp_ Forward Relay: In this type of relay, information arrived at one node including signal and noise is only amplified and forwarded. It is obvious that in this case, this operation is done quickly and in addition to the signal amplifying, the noise is also amplified.

Signal + noise → amplification of the both

Amp_ Forward Relay

Decode_ Forward Relay: In this type of relay, the information arrived at a node, including signal and noise is separated after being opened; then, the noise receives it and the raw signal is forwarded again. In this method, the operation is more time consuming, but as the noise is received, the forwarded signal has more quality.

Signal + noise → noise remove + raw signal amplification

Decode_ Forward Relay

After discussing the above issues, we can create limitations: In order to forward messages reliably, we provide the method in which nodes with a higher security level are allowed to do the broad cast with a high value and use two types of relay. And nodes with low ratings from security point of view, will have limited allowance and access. In this case, a new and insecure node is not allowed to do the broad cast and or is only allowed to do a very low multi cast. In addition, in using relays, it is only allowed to use the amp-forward relay and is not allowed to do the decoding.

The secure node: broad cast: high
Relay: amp-forward relay: is done
Decode-forward relay: is done
Insecure node: broad cast: low
Relay: amp-forward relay: is done
Decode-forward relay: is not done

5. Conclusion

Today, accuracy and security in Ad Hoc networks is one of the main challenges in these networks. In this paper, it is attempted to solve this problem by presenting some strategies [11] through which the accuracy and security of the Ad Hoc network is improved. In this case, information and package exchange is done by secure nodes more and consequently, insecure and selfish nodes are exposed in the routing and messages transfer less, leading to the isolation of nodes and finally enhancing the network's trust. In addition, using the mechanism of forwarding a virtual package, a proper framework is created for the evaluation and testing of new nodes in the network.

References

[1] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys And Tutorials, Volume 13, No 4,Fourth Quarter 2011. http://dx.doi.org/10.1109/SURV.2011.092110.00088.

[2] Jing Tian, Lu Han, Kurt Rothermel, "Spatially Aware Packet Routing for Mobile Ad Hoc Inter-Vehicle Radio Networks", IEEE, 2003.

[3] Bimal H Patel, Parth D Shah, Harikrishna B Jethva and Nishidh Chavda, "Issues and Imperatives of Ad hoc Networks", International Journal of Computer Applications, Volume 62, No.13, January 2013.

[4] Jacob Abraham, V.Arun Prasath and G.Michael, "A Survey of Intrusion Detection for Ad hoc Network", Journal of Global Research in Computer Science, April 2013.

[5] P.Ramesh Kumar, G.Nageswara Rao and P.Rambabu, "Packet Classification Methods to Counter Jamming Attacks in Ad hoc Networks", International Journal for Development of Computer Science & Technology, August and September 2013.

[6] P. Narendra Reddy, CH. Vishnuvardhan and V. Ramesh, "Routing Attacks in Mobile Ad hoc Networks", International Journal of Computer Science and Mobile Computing, May 2013.

[7] Seung-Jun Kim and Georgios B. Giannakis, "Optimal Resource Allocation for MIMO Ad hoc Cognitive Radio Networks", IEEE Transactions ON Information Theory, Volume 57, No.5, May 2011.

[8] Yi Song and Jiang Xie, "ProSpect: A Proactive Spectrum Handoff Framework for Cognitive Radio Ad hoc Networks without Common Control Channel", IEEE Transactions on Mobile Computing, July 2012. http://dx.doi.org/10.1109/TMC.2011.140.

[9] Maxim Raya, Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, 2007.

[10] Raffaele Bruno, Marco Conti, Enrico Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks", IEEE Communications Magazine, March 2005. http://dx.doi.org/10.1109/MCOM.2005.1404606.

[11] Sushant Sharma, Yi Shi, Y. Thomas Hou and Sastry Kompella, "An Optimal Algorithm for Relay Node Assignment in Cooperative Ad hoc Networks", IEEE/ACM Transactions on Networking (TON), June 2011.