Risk of Attack Coefficient Effect on Availability of Ad-hoc Networks

Diman Zad Tootaghaj, Farshid Farhat, Mohammad-Reza Pakravan, Mohammad-Reza Aref

Department of Electrical Engineering, Sharif University of Technology, Tehran , Iran

{diman_zad, farhat}@ee.sharif.edu
{pakravan, aref}@sharif.edu

Abstract— **Security techniques have been designed to obtain certain objectives. One of the most important objectives which all security mechanisms try to achieve is availability which insures that network services are available when required by various entities in the network. But there has not been any certain parameter to measure this objective in network. In this paper we will consider the availability parameter as a security parameter in ad-hoc networks. However this parameter can be used in other networks as well. We will also present the connectivity coefficient of nodes in network which shows how important is a node in network and how much would network damage if a certain node in network will be compromised.**

Keywords- Ad-hoc Networks, Security, Availability, Connectivity.

I. INTRODUCTION

There has been considerable effort recently to prevent security attacks in wireless ad-hoc networks but there has not been any specific definition for risk analysis of these networks under such attacks. In this paper we propose a function to measure importance of nodes in network. First we introduce essential goals which a security mechanism should support in section 2. In section 3 we present connectivity coefficient which can be calculated in two methods, series connectivity coefficient and parallel connectivity coefficient. In section 4 another parameter is introduced called risk of attack and simulation results of our own simulator, Mobile Ad-Hoc Network Simulator (MANETS) are given in section 5.

II. FUNDAMENTAL CONCEPTS

In creating a security mechanism, we must first consider what to achieve. Most security professionals like to describe a secure network as one that supports five essential goals [1]:

- Confidentiality ensures private data will remain private.

- Integrity ensures that the data the user is reading is in its original, authorized, unmodified form.

- Authentication ensures that users are who they claim.

- Non-repudiation ensures that a party can't falsely deny its actions nor entities falsely claim commitments from other entities.

- Availability ensures data is available when user expects it.

Availability is one of the most important parameters in creating a secure network. Because losing availability means losing resources of the system and losing connection. One of the simplest ways to disrupt a network is to simply render the network unavailable. Furthermore most routing attacks in ad-hoc networks attack availability of networks. So it would be very useful to define a parameter which measures availability of network.

III. CONNECTIVITY COEFFICIENT

Assume that the network topology is described as a graph G which is an ordered pair of disjoint sets (N, E) where $E \subseteq N \times N$. Set N is called the vertex, or nodes in network, while set E is the edge set of graph G [2]. Typically, it is assumed that every two nodes which are in radio range of each other are connected by a bidirectional link which is edges of network graph. In this paper we label every node and every edge in the graph with a specific weight. Then we present two methods to describe connectivity coefficient of nodes in network. The first method is called series model. Because in this model weights are summed up similar to calculating total resistance of series resistors in a circuit. The second method called parallel method is so called because it is similar to calculating total resistance of parallel resistors. Next we define each method in details.

A. Series Connectivity Coefficient

Assume network graph of figure 1. The weight of each node is defined to be the number of its neighbor nodes or equally its degree in graph model. Also assume that weight of every edge in the graph is obtained by multiplying its two ending nodes' degree. Next we define pre-connectivity of G as:

$$Pre\ connectivity\ of\ G \triangleq Pre-C(G) = \sum_{for\ E_i \in E} W_{E_i} \qquad (1)$$

Where W_{E_i} is the weight of edge E_i . Then series connectivity coefficient is defined

$$Series\ Connectivity\ Coeficient\ of\ G \qquad (2)$$
$$\triangleq Series\ CC(G) = \frac{Pre-C(G)}{Pre-C(G_n)}$$

Where $G_n = (N, E)$ is a complete graph of order n shown in figure 2 such that $|N| = n$ and $(u,v) \in E$ for any two distinct nodes $u, v \in N$. Note that $Pre-C(G_n)$ is a limited value for any graph with n nodes which will normalize $Pre-C(G)$ to Series Connectivity Coefficient of G. We can compute $Pre-C(G_n)$ as follows:

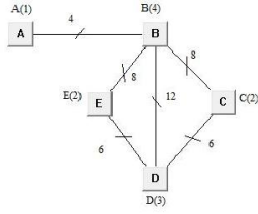$$Pre-C(G_n) = (n-1)^2 \binom{n}{2} \qquad (3)$$

Figure 1. A sample network topology and weight of vertexes and edges in Series Connectivity Coefficient
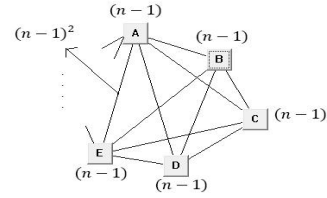

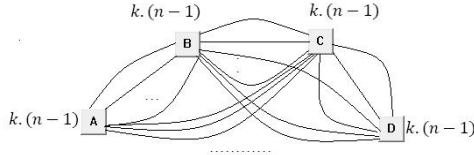Figure 2. A complete graph of order n and its weights

Figure 3. Complete graph of which there are k edges between two nodes
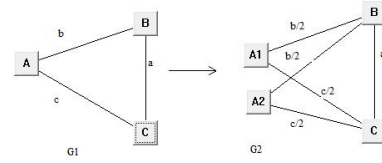

Figure 4. Decomposition of network graph don't change connectivity coefficient in Series model $CC(G_1) = CC(G_2)$

For example the Series Connectivity Coefficient of figure 1 can be computed as

$$Series\ CC(G_1) = \frac{4 + 8 + 8 + 6 + 12 + 6}{(5-1)^2 \binom{5}{2}} == 0.275 \quad (4)$$

Note that in this method we can consider the following properties:

a) We can assume that the network is a directed graph or we can have more than one edge between two nodes. In this case we should consider all cases and the largest value of pre-connectivity is assumed to be the calibration value. For example if we can have the maximum number of k edges between any two nodes (fig. 3), then the calibration factor is defined as

$$Pre - C\big(G_{n,k}\big) = k(k.(n-1))^2 \binom{n}{2} \quad (5)$$

b) We define Importance coefficient of links as follows

$$Importance\ Coefficient\ of\ E = IC_E$$
$$\triangleq \left(1 - \frac{w_E}{Series\ CC(G)}\right) or \quad \frac{1}{w_E} \quad or \quad \frac{Series\ CC(G)}{w_E} \quad (6)$$

The last one is the most interesting, as we can see the following equation is satisfied

$$\frac{1}{IC_{E_1}} + \frac{1}{IC_{E_2}} + \cdots + \frac{1}{IC_{E_n}} = 1 \quad (7)$$

c) This method describes mean connectivity value for a specific class of graphs (with a specified order of graph and specific number of edges). But we should consider variance of variations of this parameter in network as well. After calculating connectivity coefficient we can use the following value as variance of connectivity coefficient in network

$$v^2 = \frac{\sum (w_{E_i} - CC(G)/n)^2}{n^2} \quad (7)$$

d) The Series Connectivity Coefficient works for disconnected graphs as well. Even if there was a single node in the graph it won't affect connectivity coefficient of network because its edge's weights is equal to zero.

e) In this method we can decompose nodes. As you can see in figure 4 weights of nodes don't change and the connectivity coefficient of G_1 and G_2 are equal.

f) Series Connectivity Coefficient could be defined $CC_V(G)$ to messure nodes importance as well by changing weights of links to weight of nodes,that sum of the degrees of the neighbors of the node(N) is the weight of the node (N).

g) Simulation results shows that series nodes importance is the upper bound approximate of the network nodes importance.

B. Parallel Connectivity Coefficient

In this method instead of using weights we use inverse weight values and we don't need any normalization factor. Computing Parallel Connectivity Coefficient is the same as computing total resistance of parallel resistors in a circuit.

$$Parallel\ Connectivity\ Coeficient\ of\ G \triangleq Parallel\ CC(G)$$
$$= \frac{1}{2}\left(\sum_{for\ E_i \in E} W_{E_i}^{-1}\right)^{-1} \quad (8)$$

The following equation shows Parallel Connectivity Coefficient of figure 5.

$$Parallel\ CC(G_1) = \frac{1}{2}(4^{-1} + 8^{-1} \times 2 + 12^{-1} + 6^{-1} \times 2)^{-1} \cong 0.545 \quad (9)$$

Parallel Connectivity Coefficient of a complete graph can be derived as follows

$$Parallel\ CC(G_n) = \frac{1}{2}\left((n-1)^2 \binom{n}{2}\right)^{-1} = 1 - \frac{1}{n} \quad (10)$$

It is obvious that as n increases $Parallel\ CC(G_n)$ approaches to one. In this method we consider the following properties:
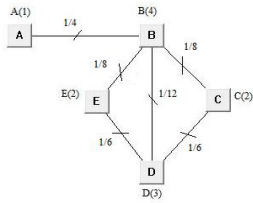
Figure 5.   A sample network topology and weight of vertexes and edges in Parallel Connectivity Coefficient
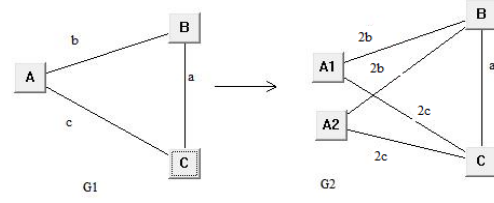

Figure 6.   Decomposition of network graph don't change connectivity coefficient in Parallel model $CC(G_1) = CC(G_2)$

a) This method does not need any normalization factor and it works for connected graph. Parallel Connectivity Coefficient of disconnected graphs is equal to zero.

b) Similar to Series Connectivity Coefficient, we can calculate variance of Connectivity Coefficient as follows

$$v^2 = \frac{\left(\sum (w_{E_i}^{-1} - CC(G))^{-2}\right)^{-1}}{n^2} \qquad (11)$$

c) Similar to the previous method we can define Importance coefficient of links as $\frac{Parallel\ CC(G)}{w_E}$.

d) Note that in this method node decomposition can be done too. As you can see from figure 6 weights of nodes don't change. But edge weights have been doubled and G_1 and G_2 have the same connectivity coefficient.

IV.   RISK OF ATTACK COEFFICIENT

In order to evaluate risk of attack a new parameter is introduced called Risk of Attack, when certain nodes in network are compromised, the graph connectivity coefficient is changed from $CC(G_1)$ to $CC(G_2)$. Where G_1 is the graph of network where none of nodes have been compromised and G_2 is the graph of network in which compromised nodes have been removed. Then Risk of is defined as follows:

$$Risk\ of\ Attack = CC(G_1) - CC(G_2) \qquad (11)$$

This parameter shows how much network will be affected under a specific attack. There have been many security attacks which can threat network functionality. Selfishness of independent nodes locally degrades network routing efficiency [3,5]. Also malicious nodes can easily corrupt the performance of the MANET by showing their Byzantine behaviors and so what is called a wormhole attack [4]. Risk of wormhole is defined as importance of wormhole link in network as considered in (6)

V.   SIMULATIONS

To investigate node importance parameter in a real network, we compare connectivity coefficient of nodes in some sample network topologies with experimental data generated by our own simulator MANETS: Mobile Ad-Hoc Network Simulator. MANETS is written in Visual C++ programming language and supports different network topologies. For the physical layer propagation model we used two-dimensional ground model. In the MAC layer we used the IEEE802.11b protocol. In order to compare performance of importance node parameter with experimental results we have simulated a

scenario in which there is a connection between every two pair nodes in network. It means we have $n(n-1)$ connections for every network which consists of n nodes.

We used sample network consisted of 50 nodes randomly placed over a 300*300 m^2 area. The coverage area of each node is 200 meters and $n(n-1)$ traffics are initiated between every two selected pairs. Ten random topologies were generated and simulations were run for every topology. The reported results are the average of these simulation runs. Simulation results show that node importance coefficient is 10% different than node importance of simulation results. But as it can be calculated locally and nodes don't need to have complete topology of network it is a valuable parameter for nodes to know about this parameter with less complexity. Furthermore we can calculate risk of wormholes using a network topology in which every two nodes in network have connection with each other and calculate risk of wormhole as

$$\frac{Number\ of\ connections\ usin\ wormhole\ link}{Number\ of\ all\ connections}$$

Simulation results show that in most cases the parameter calculated by $Series\ CC(G)/W_E$ is 15% of the real parameter calculated by simulation.

VI.   CONCLUSION

This paper introduces a new topology-based approach to measure importance of nodes in network and evaluate risk of different attacks in network including selfishness and wormhole attacks. Our proposed scheme complexity to calculate node importance is lower than the practical complexity. Simulation results show the theoretical results getting from series/parallel methods are near the real values.

REFERENCES

[1] Anjum, F. and Mouchtaris, P., "Security for Wireless Ad Hoc Networks", John Wiley &. Sons, Inc., ISBN 978-0-471-75688-0, 2007.

[2] Bollob´as, B., Modern Graph Theory, Springer, New York (1998).

[3] I. B. Wang, S. Soltani, J. Shapiro and P. Tan, "Local detection of selfish routing behavior in ad hoc networks", Proceedings of 8th international symposium of parallel architectures, algorithms and networks, IEEE, 2005.

[4] A. Perrig, Y-C Hu, D. B. Johnson, Wormhole Protection in Wireless Ad Hoc Networks, Technical Report TR01-384, Dep. Of Computer Science, Rice University.

[5] F. Farhat, M. R. Pakravan, M. Salmasizadeh, M. R. Aref, "Locally Multipath Adaptive Routing Protocol Resilient to Selfishness and Wormholes", ISPEC 2010, LNCS Volume 6047/2010, 187-200, 2010.