ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

A Graph Theoretic Modeling for Securing Link Layer in Mobile Ad Hoc Networks

Mnar Saeed Alnaghes, Fayez Gebali

Abstract - The increased usage of wireless ad-hoc networks (MANET), which is a collection of wireless mobile nodes that form a dynamic network without the need for infrastructure or centralized points, in many different applications has opened the door for many security challenges. In recent years, securing and protecting communications between mobile nodes in MANETs have become an active research field. The vast majority has only focused on providing authenticity of the route and mostly ignored the availability of malicious nodes in the environment. The aim of this work is to explore the effectiveness of malicious nodes in MANETs considering the Request-to-Send (RTS) / Clear-to-Send (CTS) protocol. It is assumed that a certain node is not listening to any RTS messages until it has a specific number of nodes within its range, and, it will have a fixed period of time before it replies a CTS message. In this paper, specific attention was paid to the security issues of a mobile ad hoc network. We propose a graph theoretic model that satisfies the basic mobility requirements of a MANET and define a mathematic analysis for the model in order to show the effectiveness of a malicious node in this network.

Keywords **- Security, Network security, MANET, RTS, CTS, Graph theory.**

I. INTRODUCTION

Mobile ad hoc network is an autonomous collection of devices that communicate with each other over wireless. This type of network is a standalone network and its functionality is established through node cooperation. Nodes which appear within each other's transmission range can communicate directly, and, they can dynamically discover each other. The network path is an open peer to peer connection between the nodes over a common frequency band, there is no fixed infrastructure, as well as, the wireless medium may be shared. The bandwidth could be limited and stringent resource constraints. MANET's features make this network vulnerable to many attacks, thus, securing communications between mobile nodes in a hostile environment is important to prevent malicious nodes from participating in a connection's path [7].

Malicious nodes use several techniques to illegally increase their throughputs and capture the channel at the expense of other normal nodes as introduced by Lolla et al. [5]. In IEEE 802.11, selfish nodes manipulate the back-off timer to increase their probabilities in having successful transmissions by simply decreasing the back-off timer value instead of following the binary backoff strategy. A node is considered malicious when it deviates from the IEEE 802.11 MAC Standard [1].

Multiple simultaneous but spatially separated transmissions are possible in the ad-hoc network [3]. Thus, the RTS/CTS mechanism is a widely used technique for packet transmission between nodes in IEEE 802.11 Medium Access Control (MAC) protocol which helps to avoid packet collisions in order to achieve high throughput. In the RTS/CTS protocol, the source informs the destination of its intention to exchange data by issuing an RTS packet, and the destination confirms this with a CTS packet, after which the source sends the payload (DATA) packet. All other nodes that recover the RTS or CTS packets are unable to transmit during some specified time interval in order to facilitate a successful RTS-CTS-DATA cycle [4].

The paper is organized as follows; Section II specifies proposed model assumption. Followed by section III where the graph theoretic model is introduced. Then, we show modeling effect of malicious node in section IV. Then, Section VI concludes the paper.

II. PROPOSED MODEL ASSUMPTIONS

In this security model, we assumed that any node in this network will not listen to any RTS request until it has a specific number of nodes within its range which is 4 nodes. In addition, the node will have a fixed period of time before it replies a CTS message, which may help in reducing the number of malicious nodes in the range. Besides, the following assumptions that were made for the analysis:

1. The network size is an L x L grid.
2. Nodes are randomly distributed across the grid points and the probability that a node is located at a particular grid point is a.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

3. Malicious nodes are randomly distributed across the available locations.
4. Every grid point can be occupied only by one node.
5. A node can talk only to its immediate four neighbors.
6. Probability that a node has a packet to send is a.

The sketch of the LxLgrid system is in Fig. 1.

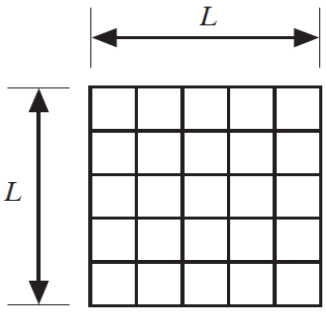

Figure 1: The L × L grid system

According to Assumption 2, the average number of nodes in the network is given by:

$$N = \alpha L^2 \qquad (1)$$

A. Establishing a route

We make two assumptions for establishing a route between a source node S located at point (i_1, j_1) and a destination node D located at point (i_2, j_2):

1. All links have the same weight or same cost.
2. Shortest distance or smallest cost route strategy is adopted.

Based on the above two assumptions, the route taken by the packets between S and D will cover a path in the region bounded by the two conditions:

$$i_2 \leq i \leq i_1, \quad j_2 \leq j \leq j_1 \qquad (2)$$

This region is indicated by the shaded rectangle in Fig. 2.

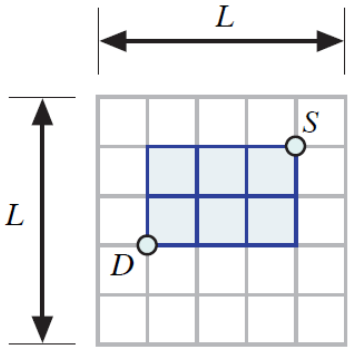

Figure 2: Source and destination nodes in the L × L grid system

It must be noted that the route between S and D can never exist outside the shaded region of Fig. 2.The number of possible routes between S and D will be discussed in Section B.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

B. Effect of Malicious Nodes in the MANET Network

Consider the source and destination nodes shown in Fig. 2. A malicious node or more could be present in the network as indicated by the red node in Fig. 3. There are two cases that can take place. First case is when the malicious node is located outside the shaded region of Fig. 3. According to the discussion in Section A, such a malicious node will have no impact on the communication between nodes S and D. The second case is when the malicious node is in the shaded region of the source and destination as shown in Fig. 3. Such a node can affect the security of the communication between S and D provided that the established path goes through the malicious node.

III. THE GRAPH THEORETIC APPROACH FOR MODELING MANETS

A. Connectivity Matrix

Assuming we have N nodes in the network, the connectivity matrix (A) is a symmetric N x N 1-0 matrix where element $a_{i,j} = a_{j,i} = 1$ when there is a link between node i and node j. It should be noted that all diagonal elements are zero, i.e. $a_{i,j} = 0$ for $0 < i \leq N$. This is to prevent self-cycles.

$$A = \begin{pmatrix} 0 & a_{1,2} & \cdots & a_{1,N} \\ a_{2,1} & 0 & \cdots & a_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N,1} & a_{N,2} & \cdots & 0 \end{pmatrix} \quad (3)$$

B. Algebra for Routing Strategy

The graph representing the network could be considered as a non-directed graph. We can study the available paths of length k between nodes by the nonzero entries of the k-th power of the connectivity matrix A. Such a strategy was used to study paths in Directed Acyclic Graphs [2] However, for non-directed graphs, the paths can be studied by a modified matrix exponentiation algorithm shown in Algorithm 1. The algorithm essentially removes all nonzero entries if they have been flagged as a path.

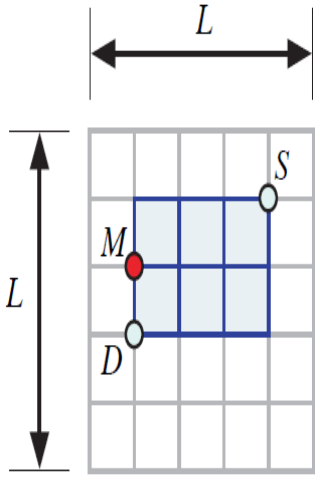

Figure 3: a malicious node appears in the route between source and destination

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

1: **Input A, k**
2: **Initialize** $B = I, F = I$
3: **for** $i =$ to k **do**
4: $B \leftarrow B \times A$
5: **for** $i = 1$ to n **do**
6: **for** $j = 1$ to n **do**
7: **if** $B(i, j) > 0$ AND F(i,j) = 1 **then**
8: $B(i, j) = 0$
9: **end if**
10: **if** $B(i, j) > 0$ AND F(i,j) = 0 **then**
11: $B(i, j) = 1$
12: **end if**
13: **end for**
14: **end for**
15: **end for**
16: **Return** $A^k \leftarrow B$

Algorithm 1: Modified connectivity matrix multiplication algorithm to obtain A^k

As an example, consider the case when N = 9. The actual node distribution is shown in Fig. 4.
The associated connectivity matrix has the form:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (4)$$

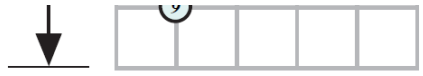

Figure 4: Example of a 9-node MANET network.

Notice that columns4 and 9 and rows 4 and 9 are all zeros to indicate that nodes #4 and #9 are isolated and cannot communicate with the other nodes.
To study all paths of length 2, i.e. two-hop paths, we look at A^2:

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

$$A^2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5)$$

We note that node #1 has a single 2-hop path to nodes #3 and #5. Node #2 has two 2-hop alternative paths to node #6. It also has a single 2-hop path to node #8.
Three-hop paths are explored through matrix A^3:

$$A^3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (6)$$

We observe that node #1 has two 3-hop paths to node #6. It also has a single 3-hop path to node #8.
Four-hop paths are explored through matrix A^4:

$$A^4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (7)$$

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

IV. MODELING EFFECT OF MALICIOUS NODES

The previous section gave us estimates of the number of k-hop paths between a pair of network nodes. The number of k-hop paths between any pair of nodes is easily estimated from the entries of the matrix A^k. Given a source node S located at point(i_1, j_1) and a destination node D located at point(i_2, j_2), we can estimate the distance between them as the Manhattan distance given by:

$$\lambda_{S-D} = |i_1 - i_2| + |j_1 - j_2| \quad (8)$$

The number of paths between S and D is estimated from the entries of matrix $A^{\lambda_{S-D}}$as:

$$r_{S-D} = a(k_1, k_2) \quad a(k_1, k_2) \in A^{\lambda_{S-D}} \quad (9)$$

where k_1 is the index or label of the source node and k2 is the index of the destination node.
Assuming a malicious node M is located at point (i_3, j_3) as shown in Fig. 3. The Manhattan distance between S and M is given by:

$$\lambda_{S-M} = |i_1 - i_3| + |j_1 - j_3| \quad (10)$$

The number of paths between S and M is estimated from the entries of matrix $A^{\lambda_{S-M}}$ as:

$$r_{S\ M} = a(k1,k3) \quad a(k1,k3) \in A^{\lambda_{S-M}} \quad (11)$$

Where k1 is the index or label of the source node and k3 is the index of the malicious node.

The probability that a packet sent from S to D is intercepted by the malicious node is given by:

$$p_a(k_1, k_2) = \beta \times \frac{|i_1 - i_2| \times |j_1 - j_2|}{L^2} \times \frac{r_{S-M}}{r_{S-D}} \quad (12)$$

The first term on the RHS is the probability β that a malicious node is present in the network. The second term on the RHS is the probabilities that the malicious node is present in the shaded are a shown in Fig.3. The third term on the RHS is the probability that sent packet is intercepted by the malicious node. The probability of an attack on packets sent from S to D is therefore given by:

$$p_a(k_1, k_2) = \beta \times \frac{|i_1 - i_2| \times |j_1 - j_2|}{L^2} \times \sum_{k_3 \neq k_1, k_2} \frac{r_{S-M}}{r_{S-D}} \quad (13)$$

A Numerical Example

To illustrate our malicious node model, we assume that a malicious node is known to be present at the location of node #5 in the network shown in Fig.4.Figure 5 illustrates this situation.

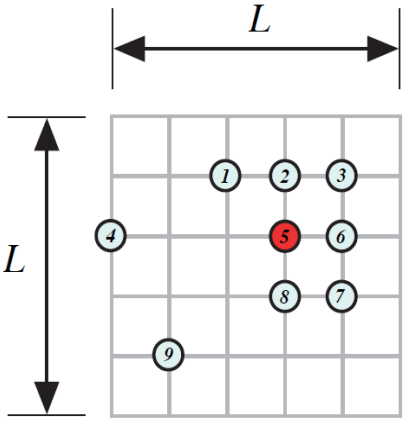

Figure 5: Example of a 9-node MANET network with malicious node located at node #5.

The malicious node at location #5 could intercept packets between node pairs such as #1–#6. It will have no impact on communications between node pairs #7–#3, for example.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

Since we know that we have a malicious node located at position #5, Eq. (13) has to be modified as:

$$p_a(k_1, k_2) = \frac{r_{S-M}}{r_{S-D}} \quad (14)$$

Table 1 shows the probability of attacks between source and destination nodes of Fig. 5.

Table 1: the probability of attacks between source and destination nodes

Destination Node \ Source Node	1	2	3	4	5	6	7	8	9
1	0	0	0	0	0	0.5	0.33	1	0
2	0	0	0	0	0	0.5	0.67	1	0
3	0	0	0	0	0	0	0	0.67	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0.5	0.5	0	0	0	0	0	0.5	0
7	0.33	0.67	0	0	0	0	0	0	0
8	1	1	0.67	0	0	0.5	0	0	0
9	0	0	0	0	0	0	0	0	0

Consistent with Fig. 3 when the malicious node is present in the zone defined by S and D, then there is a nonzero probability of an attack. This is evident from the Table 1 such as for node #1 and #6 or #7. Of course if the source or destination node is itself the malicious node (#5), then the probability of an attack is exactly 1. For a fixed data source, i.e. looking at a certain table column, we note that the probability of an attack increases as the destination node is closer to the malicious node. Likewise, for a fixed destination, i.e. looking at a certain table row, we note that the probability of an attack increases as the source node is closer to the malicious node.

V. CONCLUSION AND FUTUREWORK

Due to the nature of MANETs functionality, there are a lot of security challenges in these networks. Security begins with an understanding of how the network needs to be secured. In this paper, we propose a graph theoretic model that satisfies the basic mobility requirements of a MANET and we considered the Request-to-Send (RTS) / Clear-to-Send (CTS) protocol for nodes to communicate with each other. We also assumed that any node will not listen to any RTS messages until it has a specific number of nodes within its range, and, it will have a fixed period of time before it replies a CTS message. In order to do the analysis, we defined a mathematic analysis for the model in order to show the effectiveness of a malicious node in this network. As part of future work, we would like to study the generic scenario with multiple misbehaving nodes in a multi-hop wireless network.

REFERENCES

[1] IEEE-SA Standards Board, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1389197, 2003.

[2] F. Gebali, Algorithms and Parallel Computing", New York: John Wiley, 2011.

[3] D. S. J. De Couto and R. Morris. "Location Proxies and Intermediate Node Forwarding for Practical Geographic Forwarding", 2001.

[4] V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, and E. Knightly, Ordered packet scheduling in wireless ad hoc networks: Mechanism and performance analysis, in Proc. of MOBIHOC02, 2002.

[5] VN. Lolla, LK. Law, SV. Krishnamurthy, C. Raishankar, D. Manjunath, Detecting MAC layer backoff timer violations in mobile ad hoc networks. in Proc. of the 26th IEEE international conference on distributed computing systems, 2006.

[6] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris. "A scalable location service for geographic ad hoc routing". in Proc. ACM/IEEE Mobi Com, 2000.

[7] C.Siva Ram Murthy and B S Manoj,"Mobile Ad Hoc Networks-Architecture and Protocols" , Pearson Education, ISBN 81-317-0688-5 ,2004.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

ACKNOWLEDGEMENT

We would like to thank the Ministry of Higher Education in Saudi Arabia and Saudi Bureau in Canada for partially supporting this research.

AUTHOR BIOGRAPHY

Mnar Alnaghes received her B.Sc. in Statistics and Computer Sciences from King Abdul Aziz University (KAAU). She is currently a grad student in the Department of Electrical and Computer Engineering at University of Victoria (UVIC) in BC Canada.

Dr. Fayez Gebali received his B.Sc. in Electrical Engineering (first class honors) from Cairo University, his B.Sc. in Mathematics (first class honors) from Ain Shams University, and his Ph.D. degree in Electrical Engineering from the University of British Columbia where he was a holder of an NSERC postgraduate scholarship. Dr. Gebali is a Professor and Chair of the Department of Electrical and Computer Engineering at the University of Victoria (UVIC) in BC Canada.