International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (GRAPH-HOC) Vol.9, No.2, June 2017

A PROPOSAL ANALYTICAL MODEL AND SIMULATION OF THE ATTACKS IN ROUTING PROTOCOLS OF MANETS: IMPLEMENTATION OF A SECURE MODEL OF MOBILITY

Karim KONATE and Abdourahime GAYE

Department of Mathematics and Computing, University Cheikh Anta DIOP, Dakar

ABSTRACT

In this work we have devoted to some proposed analytical methods to simulate these attacks, and node mobility in MANET. The model used to simulate the malicious nodes mobility attacks is based on graphical theory, which is a tool for analyzing the behavior of nodes. The model used to simulate the Blackhole cooperative, Blackmail, Bandwidth Saturation and Overflow attacks is based on malicious nodes and the number of hops. We conducted a simulation of the attacks with a C implementation of the proposed mathematical models.

KEYWORDS

Routing, Security, Attacks, Mobility, Modelling, Simulation, Mobile ad hoc

1. INTRODUCTION

Today ad hoc networks (MANET) are a more and more adopted technology. This is mainly due to the continuing development of networks, the growing need for mobility, miniaturization of networking devices, universal access to information and its sharing.

In MANETs the other intermediate network nodes will be used as gateways or relays. Indeed, this routing is a problem of optimization under such constraints like topology changes, volatility of links, limited storage and processing capacity, low bandwidth, low power level in batteries, etc. These binding characteristics make MANETs very vulnerable to attacks comparing to wired networks or infrastructure-based wireless networks.

The document is structured: we presented in the first some of the attacks and the countermeasures met in the .MANET, in the second we proposed a mathematical model and the end we implanted our analytical model.

2. BACKGROUND

An attack is an action which aims at compromising the security of the network. They are many and varied in these MANET:

BlackHole attack: consists in dropping some routing messages that node receives [1, 2, 3, 4, 5]. It was declined in several particularity alternatives, having different objectives, among which we can quote:

- Routing loop, which makes it possible for a node to create loops in the network ;
- Grayhole, which lets pass only the packages of routing and diverts the data ;
- Blackmail, which makes it possible for a node attacker to isolate another node.

The selfish attack: consists in not collaborating for the good performance of the network. We can identify two types of nodes which do not wish to take part in the network. Defective nodes i.e. do not work perfectly. Those which are malevolent, it is those which intentionally, try to tackle the system: attack on the integrity of the data, the availability of the services, the authenticity of the entities (denial-of-service, interception of messages, usurpation of identity, etc). Selfish nodes are entities economically rational whose objective is to maximize their benefit [4, 5, 10, 11].

Overflow routing tables: consists of malicious nodes to cause the overflow routing tables of nodes being used as relay [1, 2, 4, 31].

Sleep deprivation: consists to make a node to remain in a state of activity and to make him consume all its energy [1, 2, 4, 31].

3. Analytical Modelling of the Attacks

In this part we make a modeling of some of these attacks like Overflow, Blackmail and Cooperative Blackhole by using mathematical tools. I chose these attacks in my analytical model because in my routing protocol which I would have to implement I would take into account these attacks i.e. I will propose a mechanism to fend off or reduce the impact of these attacks In the article [24, 25, 31], the author models the Blackhole attack whose node tries to integrate the network and tries to provide an optimal way and to be able to reject the packets, not to broadcast them during the reception. He goes by the size of the network and the attackers to evaluate the waste of time. For Overflow, Blackmail, Cooperative Blackhole, the attackers try to integrate the network and to create the fictitious or nonexistent connection so as to cause a loss of the packets during the transmission. This approach which is based on malicious nodes can be suited to our simulation of the above mentioned attacks. In the case of our modelling of the attacks (Overflow, Blackmail, Cooperative Blackhole), we consider an ad hoc network whose size is equal to N nodes.

We suppose that among N nodes, the A (A<N) nodes of these nodes are malicious nodes. We note by p the probability that attacker node is randomly selected such as p = A/N. Take the example of a way crossing h hops [24, 25, 29]. If the selected nodes represent a sample random of N nodes of the network, then the probability so that a way doesn't contain attacker nodes is $(1-p)^h$. We calculate the percentage in normal transmission according to the time alternated between the periods of success transmission and the periods of failure transmission. In particular, we note the time to live of a route determined by factors like the speed and the density of nodes. It is a form of D/V where D is the distance or the range from emission and V the transmission speed for node. When a route is defective the fact of mobility, a certain number of delay is shown during the repair of the route. We note three types of delay [24, 25, 29]:

- Tdiag to diagnose the route ;
- TRL to send a route request ;
- TRR to receive a route replay.

First, duration Tdiag is noted to diagnose that the route is broken (sending of Route Error, Hello.). Then, the request for a new route can be delayed for duration of limitation so as to attenuate the impact of flood of the route requests of malicious nodes. We note this time by TRL, which indicates the minimum time between the route requests authorized by the routing protocol. Finally, the node must wait to receive one or more messages of route replay; this slot time is noted by TRR. After these three phases, node begins to send the data on the new route. However, the new route comprises at least attacker node with a probability $1-(1-p)^h$. If such is the case, the transmission is blocked and node must redo these three delays before testing again. It should be noted that even if victim node makes sure that the new route does not contain defective routes, the new route can contain attacker node. Thus, the node leaves the phase output zero (before the transmission of the data) only after it established successfully a route without attacker node. In general, a protocol can change timers granted to the number of attempts. Either n the number of attempts at route request, T^n_{RL} indicates the duration of limitation's rate given immediately before the nth attempt. Thus, we note E (T0) the anticipated total time of output zero, i.e., total time wasted to find a new route which doesn't contain attacker node (time wasted to find legitimate routes), is given in [24, 25, 29, 31] and is the form of:

$$E(T_0) = \sum_{n=1}^{\infty} \left(\sum_{j=1}^{n} E\left(T^j_{diag}\right) + \sum_{j=1}^{n} E\left(T^j_{RL}\right) + \sum_{j=1}^{n} E\left(T^j_{RR}\right) \right) \left(1 - (1-p)^h\right)^n$$

$\left(\sum_{j=1}^{n} E\left(T^j_{diag}\right) + \sum_{j=1}^{n} E\left(T^j_{RL}\right) + \sum_{j=1}^{n} E\left(T^j_{RR}\right) \right)$ is the lost time for a number of attempts equals to n.

To simplify, we suppose that we have the same number of attempts i.e. .the same n for group of E(Tj) and we have :

$$E(T_0) = \sum_{n=1}^{\infty} n\left(E\left(T_{diag}\right) + E\left(T_{RL}\right) + E\left(T_{RR}\right)\right)\left(1 - (1-p)^h\right)^n$$

The percentage in transmission standardized i.e. time for the normal transmission over total time wasted to find a new route for a flow is given by:

$$\bar{D} = \frac{\bar{E}(T_L)}{E(T_L) + E(T_0)}$$

Under the terms of what precedes and of the assumptions we have the formula represented by:

$$D = \frac{E(T_L)}{E(T_L) + \sum_{n=1}^{\infty} n\left(E\left(T_{diag}\right) + E\left(T_{RL}\right) + E\left(T_{RR}\right)\right)\left(1 - (1-p)^h\right)^n}$$

4. MODELLING OF THE MOBILITY

Adding a mobility aspect to the ad hoc network is equivalent putting movement in known environment the nodes of the network. The representation of mobility varies enormously according to the environments considered and some mobility models were developed to cover the diverse behaviors. Among the models, we can quote Random WayPoint, Random Direction, Boundless Area Simulation and Gauss-Markov, RPGM (Reference Not Group Model).

A mobile ad hoc network is an autonomous system of mobile nodes connected by wireless links. Each node in the network can be in one of the four states: the node moves and its neighbors fixed, the node is stable and its neighbors move, the node and its neighbors are moving, the node and its neighbors are motionless [26, 27, 28].

To base itself on this simple and frequent report, we can define our mobility measure by the mobility degree of the nodes in the network which will be evaluated with discrete and regular time intervals. For each node, the mobility degree value represents at the moment T the variation undergone by its neighbors compared with moment T-1. Thus, the nodes which leave and/or join the node neighborhood influence on the evaluation mobility degree of the concerned node. Mobility is locally quantified and doesn't depend on the concerned node localization [27, 28, 29, 31].

If we pose M the mobility of node A at the moment T, NbNodes the total nodes number at moment T-1, NbNodesIn the integrated nodes number and NbNodesOut the left nodes number the coverage area of node A during the time interval of Δt duration (in the interval [T-1, T]), we can quantified M by [26, 27.28, 29, 31]:

$$\boldsymbol{M(A,t) = \frac{NbNodesIn(t)+NbNodesOut\ (t)}{NbNodes(t-1)}}$$

In order to control the metric behavior that we defined and to make it adapt to the various environments, we will define a new mobility parameter λ which makes it possible the metric flexible. Thanks to this parameter λ, we can classify the mobile environments as follows [26, 27.28] :

- an environment incoming flow is important: λ<0,5;
- an environment where outgoing flow is important: λ>0.5;
- a balanced environment where the nodes are same chance to leave or join the coverage area each other: λ=0.5.

We can formally quantify the mobility degree by:

$$\boldsymbol{M_i^{\lambda}(t) = \frac{\lambda NbNodesIn_i(t)+(1-\lambda)NbNodesOut_i(t)}{NbNodes_i(t-1)}}$$

Since the time intervals are discrete and regular, we can use the diagnostic route time and the time of waiting to receive replay like our interval i.e. $t \in [T_{diag}, T_{diag}+T_{RR}]$.

If M is the network average mobility measure in the regular time intervals and N the total nodes number in the network, we have [.28, 29, 31]:

$$\boldsymbol{M_{\lambda}(t) = \frac{1}{N}\sum_{i=0}^{N-1} M_i^{\lambda}(t)}$$

If we take into account of this network mobility metric that we defined, the expression of D associated with the mobility can write as:

$$\boldsymbol{D_M = D * M_{\lambda}(t)}$$

$$D_M = \frac{D}{N}\sum_{i=0}^{N-1} \frac{\lambda NbNodesIn_i(t) + (1-\lambda) NbNodesOut_i(t)}{NbNodes_i(t-1)}$$

If we suppose that $NbNodes \cong N$ then

$$D_M = \frac{D}{N^2}\sum_{i=0}^{N-1} \lambda NbNodesIn_i(t) + (1-\lambda) NbNodesOut_i(t)$$

5. Simulation of the Model

To make our simulation we fixed Etl=10 S, Tdiag=2 S, Trl=2 S, Trr=1 S because these values are the default values of the routing protocol DSR and which represent the time to live of the route respectively, the period of diagnosis of the defective routes, the interval of the requests for route and the latency of the route replay [24, 25, 29, 30]. These various variables are defined by the protocol of selected routing. The following table gives the parameters of the analytical model simulation.

Table 1. The simulation parameters of the analytical model

Number of nodes	N
Probability of malicious nodes	P
Number of hops	H
Number of join neighbor nodes	NbIn
Number of left neighbor nodes	NbOut
Mobility coefficient λ	$\lambda < 0{,}5$; $\lambda > 0{,}5$; $\lambda = 0{,}5$
control times	T_{diag}=2 S, T_{rl}=2 S, T_{rr}=1 S

Figure 1 gives a variation of the percentage of transmission in time in the presence of attacker nodes.

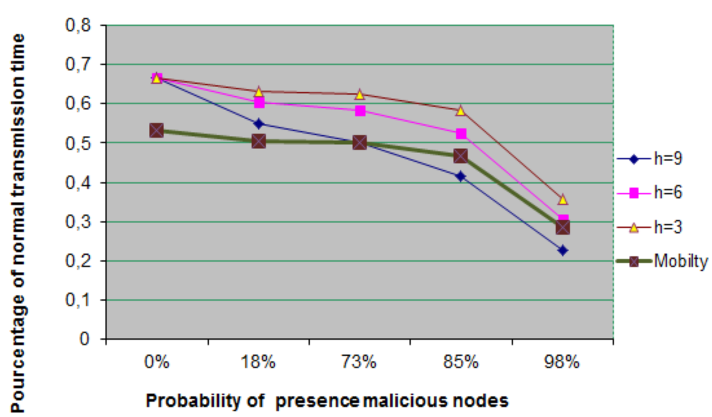


Figure 1. Impact of the attack and the length of route on the normal transmission time

For a number of hops equals to 9 when the fraction of malicious node is 0, the 68% of time are spent for the transmissions which succeed and this rate decreases and reaches the 49% when the fraction is of 0.73 and with a fraction equal to 0.98 this rates decreases and reaches the 20%. That can be explained owing to the fact that when one selects malicious nodes, the lost time

increases because it will have a delay shown for the new discovery of the routes and waiting of the answer's messages. For a number of hops equals to 6, with a fraction of malicious nodes equal to 0.73 the time spent for the transmissions which are successful is of 58% and for this fraction when the number of hops is equal to 3, the rate in time used is 63 %. Thus we note a reduction in the rate when the number of hops increases. That finds its explanation of the increase in the time of transmission. On the other hand in comparison with the normal transmission time and the total time of transmission which decreases. We vary h i.e. the number of hops to highlight the characteristics of these MANETs which is the change of topology due to the mobility of nodes.

6. ACKNOWLEDGEMENTS AND DISCUSSIONS

The world needs more and more mobility, the access and the sharing of information. This mobility materializes by the miniaturization of the peripherals (PDA, digital camera, mobile phone.). This equipment is characterized by modest computing capacities and storage and also their energy autonomy. By taking account of the mobility which is defined by a measurement M, we notice for example with 0% of malicious node probability the transmission rate is approximately 52% and if the probability is approximately 18% this rate borders on the 50%, is relatively low difference compared to malicious nodes rate. That finds its explanation on the one hand by the fact that if topology changes due to mobility the nodes accuse a delay during the establishment of their routes what influenced the normal transmission. One the other hand the nodes that we detected as malicious are also mobile nodes so that even if we take in account the mobility the rate of transmission undergoes the same variation with the malicious nodes probability.

In addition for the distribution we noticed that the items (60/10), (50/7) and (95/50) are points of our figure i.e. 7% of probability of presence malicious nodes produce approximately 50% with the mobility of normal transmission, 10% of probability of presence malicious nodes produce approximately 60% with the mobility of normal transmission and 95% of the malicious nodes give 50% of transmission, we can deduce from it that our model follows a Pareto distribution.

7. CONCLUSIONS

In our work, we modelled the mobility and the attacks by using mathematical model to see the impact of the transmission time. We implemented our model in order to make evaluations of performance. The derived metric mobility is based on integrate parameters coming from the graph theory models. These metric exits of the graphs models make call to the parameters characterizing the links state, the rate of changed link states, the link duration, the average duration way, which will be able to have an impact on the error count route. The number of received error messages route can cause two interpretations according to the origin of the element which transmits the message. We choose these metric according to the characteristics MANET.

REFERENCES

[1] Shikha Jain. Security Threats In Manets. International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.

[2] Preeti Gulia, Sumita Sihag. Review and Analysis of the Security Issues in MANET. International Journal of Computer Applications, Volume 75 - Number 8, 2013.

[3] Curtmola Reza, “Security of Routing Protocols in MANET”. 600.647-Advanced Topics in Wireless Networks,February 2007, pages 26.

[4] Amandeep Kaur, Dr. Amardeep Singh. Security Attacks in Mobile Ad-hoc Networks. International Journal of Science and Research (IJSR), Volume 3 Issue 5, May 2 014

[5] Chen Ruiliang,Snow Michael,Park Jung-Min,M. Refaei Tamer,Eltoweissy Mohamed, “Defense against Routing Disruption Denial-of-Service Attacks in MANET”, Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksburg,VA, USA, November 2005, pages 15.

[6] A.Rajaram,Dr. S. Palaniswami, “The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks”, (IJCSE) International Journal on Computer Science and Engineering Vol.02,No.02,2010,400-408. Anna University Coimbatore, India, March 2010, pages 9.

[7] T.V.P.Sundararajan et Dr.A.Shanmugam, “Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET”, Sathyamangalm-638401, Tamilnadu, India, May 2009, pages 14.

[8] Kevin Hoffman,David Zage,and Cristina Nita-Rotaru, “A Survey of Attack and Defense Techniques for Reputation Systems”, Department of Computer Science and CERIAS Purdue University, April 2008, pages 19.

[9] Pietro Michiardi, “Cooperation in the ad hoc networks: Application of the evolution and game theory within the framework of imperfect observability”, Institute Eurecom 2229, road of the Peaks LP 19306904 Sophia-Antipolis, France, July 2006, pages 17.

[10] Michiardi Pietro and Molva Refik, “CORE: A Collaborative Reputation Mechanism to enforce node cooperation in MANET”, European Wireless Conference, November 2003, pages 15.

[11] Hu Jiangyi, “Cooperation in Mobile Ad Hoc Networks”, Computer Science Department Florida State University, January 2005, pages 23.

[12] Buttyan Levente and Hubaux Jean-Pierre, “Nuglets: a virtual Currency to Stimule Cooperation in Self-Organized Mobile Ad Hoc Networks”, Institute for Computer Communications and Applications Department of Communication Systems Swiss Federal Institute of Technology Lausanne, 18 January 2001, pages 15.

[13] Yan Zheng, Zhang Peng,Virtanen Teemupekka, “Trust Evaluation Based Security Solution in Ad Hoc Networks”, Helsinki University of Technology, Finland, December 2003, pages 14.

[14] Xue Xiaoyun, “Security mechanisms for ad hoc routing protocols”, Computer Science and Network Department, ENST, thesis September 2006, pages 234.

[15] Pietro Michiardi and Refik Molva, “Analysis of Coalition Formation and Cooperation Strategies in MANET”, Institut Eurecom May 2004, pages 28.

[16] Levente Buttyan and Jean-Pierre Hubaux, “Report on a Working Session on Security in Wireless Ad Hoc Networks”, Laboratory for Computer Communications and Applications Swiss Federal Institute of Technology-Lausanne(EPFL), Switzerland, September 2002, pages 17.

[17] Pietro Michiardi , Refik Molva, “Game theoretic analysis of security in mobile ad hoc networks”, Institut Eurécom Research Report N°RR-02-070, juin 2002, pages 10.

[18] Hu Yih-Chun,Perrig Adrian,Johnson David B, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, INFOCOM 2003, pages 11.

[19] Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis, "Securing AODV Against Wormhole Attacks in Emergency MANET", Multimedia Communications,Wireless Multimedia and Networking(WMN) Research Group Kingston University London, July 2009, pages 7.

[20] Shang-Ming Jen 1,Chi-Sung Laih 1 and Wen-Chung Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET"

[21] Payal N. Raj,Prashant B. Swadas, "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET", IJCSI International Journal of Computer Science Issues, Vol.2, Computer Engineering Department, SVMIT Bharuch, Gujarat, India, September 2009, pages 6.

[22] Ramaswamy Sanjay,Fu Huirong,Sreekantaradhya Manohar,Dixon John and Nygard Kendall, "Prevention of Cooperative BlackHole Attack in MANET", Department of Computer Science,IACC 258 North Dakota State University, Fargo, ND 58105, March 2003, pages 7.

[23] Hesiri Weerasinghe and Huirong Fu, "Preventing Cooperative BlackHole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Application Vol.2,No.3, Oakland University Rochester MI 48309 USA, June 2008, page 16.

[24] Aad Imad, Hubaux Jean-Pierre, Knightly Edward W. Impact of Denial of Service Attacks on Ad Hoc Networks. DoCoMo Euro-Labs EPFL Rice University Munich, Germany Lausanne, Switzerland Houston, TX, July 2007, pages 14.

[25] Aad Imad, Hubaux Jean-Pierre, Knightly Edward W. Denial of Service Resilience in Ad Hoc Networks; MobiCom'04, Sept. 26Oct. 1, 2004, Philadelphia, Pennsylvania, USA, pages 14.

[26] Bécaye DIOUM, Effetcs of the mobility on the routing protocoles in Ad Hoc Networks, University of Mouloud Mammeri of Tizi Ouzou (Algeria) 2007

[27] Kamal OUDIDI, Routing et Quality of Service in spontaneous wireless network, university of Mohammed V, juilly 2010

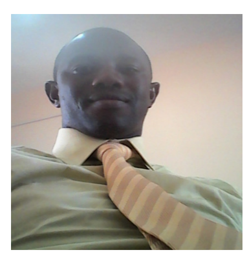
[28] Cholatip YAWUT, Adaptation of the mobility in Ad Hoc Networks, juilly 2009

[29] Dr K KONATE, A GAYE: Analysis of Attacks in mobile ad hoc networks: Modeling and Simulation. 2nd International Conference on Intelligence Systems, Modeling and Simulation (ISMS2011), ISBN 978-0-7695-4262-1 Kuala Lumpur (Malaysia) January 2011.

[30] [48]: David Joyner, Minh Van Nguyen, Nathann Cohen; Algorithmic Graph Theory, Edition Version 0.7-r1908 December 2011, pages 310

[31] GAYE Abdourahime, Dr Karim KONATE: Attacks analysis and countermeasures in routing protocols of mobile ad hoc networks,COMPUSOFT, An international journal of advanced computer technology (IJACT),ISSN: 2320 – 0790, December 2014

Authors



Dr GAYE Abdourahime Student Researcher

Laboratory of Network and Telecommunication

Doctorate Institute of Mathematics and Computing

University Cheikh Anta DIOP, Dakar

Tutor of Virtual University Senegal (UVS)