Performance Analysis of Gray Hole Attack under AODV Protocol for Mobile Ad-hoc Network.

Mahendra P. Sharma[1], Prof. (Dr.) D.K Chauhan[2]
[1]Reserch Scholar-CSE, NIU Gr. Noida, India
[2]Professor-Electrical Engg, NIU Gr.Noida, India

Abstract:
The mobile ad-hoc network (MANET) is one of the most recent active areas and has received special attention due to its self-configuration and self-maintenance capabilities. Early studies included a friendly and collaborative environment, such as focusing on wireless access and multi-stop routing issues. Recent wireless surveys has found that wireless MANET has security attacks problems over traditional wired and wireless networks [1, 2]. In this paper we analyse grayhole attack that executed under the NS2 plateform run on the linux operating system. The analysis form with some set of nodes and whole execution focused on three parameters i.e. E2E, PDR and Throughput.

Keywords: *AODV-Adhoc On demand Distance Vector,DoS- Deniel of Services,MANET- Mobile Adhoc Network,E2E-End to End Delay,PDR-Packets Delay Response, WLANs- Wireless Local area Networks,*

I. Introduction

Due to the fact that MANET is a group of nodes that form a temporary network without centralized administration, the nodes have to communicate with each other based on unconditional trust. This characteristic leads to the consequence that MANET is more susceptible to be attacked by inside the network while comparing to other type of networks. Practically, MANET could be attacked by several ways using multiple methods; before going to deeper investigation, it is necessary to classify security attacks within the context of MANET [5,6]. Recent research on MANET shows that the MANET has larger security issues than conventional networks. Any security solutions for static networks would not be suitable for MANET. Singh et al, discussed several types of attacks that can easily be performed against a MANET. Many researchers define several algorithms for MANETs is well established with many works improving on requirement of networks, each give an overview of some of the difficulties of implementing MANETs. [2,4] Therefore, security in MANETs is the most important concern for the basic functionality of network. A MANETs is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources[10]. In this paper simulation is executed under the NS2 plateform run on the linux operating system.The whole excution divide in three phase under the primary where no attack come into the setup. Secondly when attack has been excuted on same setup and lasty when is has been detected using the predictive algorithms.

II. Security Attacks

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data (Gagandeep (2012), Sachan (2011)). Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups.

III. MATHEMATICAL MODELING

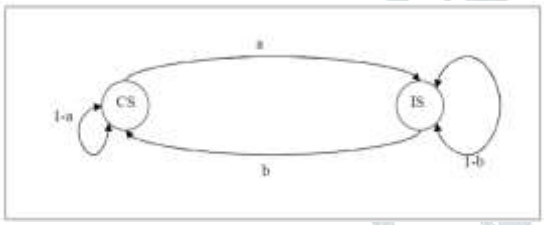
A mathematical modeling is required to model the behavior of the normal and malicious node in the network. Markov process is presented to model and analyze the stochastic properties of a node's behavior.

Modeling and Analysis of Node Misbehavior

In this paper, it is assumed that all nodes are uniformly distributed over a two dimensional area. The transmission radius r is same for all the nodes in the network. A node v is called as neighbor node of u, if and only if, the transmission distance between them is ≤r. we consider only two types of nodes called cooperative and black hole nodes denoted by N_C and N_B respectively. Cooperative nodes are those nodes that comply with the routing protocol in route discovery and data forwarding processes. Therefore we use M (N) to denote a network with the node set N, where $N=N_C \cup N_B$.

Stochastic Properties of a Node's Behavior

A random process or a stochastic process is defined to be a Markov process if given the value of X (t), the value of X (v) for v > t does not depend on the values of X (u) for u < t (Christian 2004). In other words, the future behavior of the process depends only on the present value and not on the past values. If the random process at time tn is in state Xn, the future state of the random process Xn+1 at time tn+1 depends only on the present state Xn and noton the past states Xn-1, Xn-2, …., X0. The sequence of states {Xn} is called a Markov chain. A node in the proposed model is viewed as having two states namely connected state (CS) and isolated state (IS). A state can be in either one of these two states based on the presence or absence of black hole neighbors. A two- state Markov process of a node is shown in Figure below. Let the probability of a node being in isolated or in connected state be represented by parameters "a" and "b" respectively.



Two state transition model of a network node

The parameters "a" and "b" for the node U at time instant k are formally defined as:

a = P [U (k) = IS | U (k-1) = CS]
b = P [U (k) = CS | U(k-1) = IS]

State	Connected	Isolated
Connected	1 - a	a
Isolated	b	1 - b

Table: Probability transition matrix for a two state Markov chain

Therefore the state of a node U at time instant k is formally given as

$U_{(K)}=\begin{cases} CS, if\ b = N_c \geq 1\ and\ a = N_B = 0 \\ IS\ , Otherwise \end{cases}$

Where, NC and NB are the number of cooperative and black hole neighbors respectively.

Poisson Model

To derive the neighbor nodes distribution Pr (D (u) =d) , we partition the network area A into N smaller grids where each grid size is equal to the node physical size and N denotes the number of nodes in area A. When the network area is much larger, then the probability that the node occupies a specific grid, say p, is very small. With large N and small p, Poisson distribution can be used to model node distribution as follows:

$\Pr(D_{(u)} = d)=\frac{\mu^d}{d!}e^{-\mu}$

Where, μ denotes the average number of nodes within the area covered by a nodes transmission range. The value of $\mu= p\pi r^2$ where $p=\frac{N}{A}$ denotes the node density in a network area A using a mobility model as random waypoint model.By applying total probability law

$\Pr(D_{(c,u)}=k|D_{(u)}=d)=\sum_{d-k}^{n-1}\binom{d}{k}(1-P_B)^k\ \frac{\mu^d}{d!}e^{-\mu}$ (Equ-1)

By using (8.12),$\Pr(D_{(c,u)}<k)$ can be obtained as follows:

$\Pr(D_{(c,u)}<k|D_{(u)}=)= \sum_{m-0}^{k-1}\sum_{d-k}^{n-1}\binom{d}{m}(1-P_B)^m\frac{\mu^d}{d!}e^{-\mu}$

$=\frac{t(k,u(1-P_B))}{t(k)}$ (Equ-2)

By substituting (Equ-2) in (Equ-1), we obtain the probability for a node to have at least k cooperative degree as follows:

$\Pr(D_{(c,u)>}\geq K) =\{1-\Pr(D_{(c,u)} < K)\}^N$

$= (1-\frac{t(k,\mu(1-P_B))^N}{T(k)})$

Where $t(\alpha,\beta)=(\alpha-1)!e^{-\beta}\ \sum_{i=0}^{\alpha-1}\left(\frac{\beta^i}{i!}\right)$ $\alpha\dot{\in}N$ denotes the incomplete gamma function and t (k)=(k-1)!denotes the complete gamma function. Therefore for fixed k, A and N, a network can have the maximum connectivity only if $P_B=0$

IV. Simulation of Grayhole attack

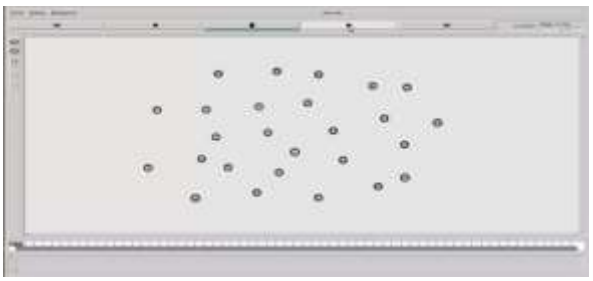


Fig 1: 25 nodes under NS2

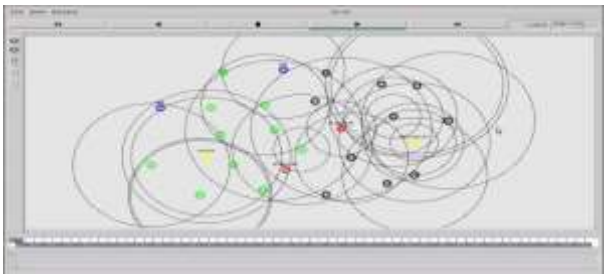


Fig 2: Start simulation of 25 nodes

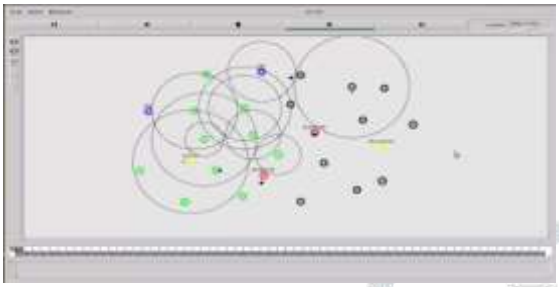


Fig 3: Drop Packet during Simulation

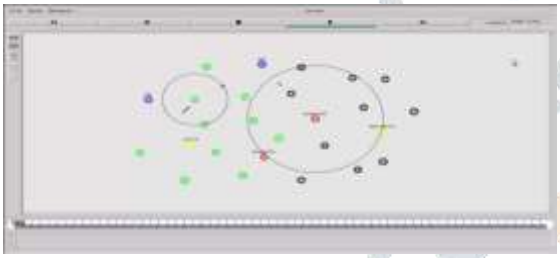


Fig 4: Data Transfer from source to destination

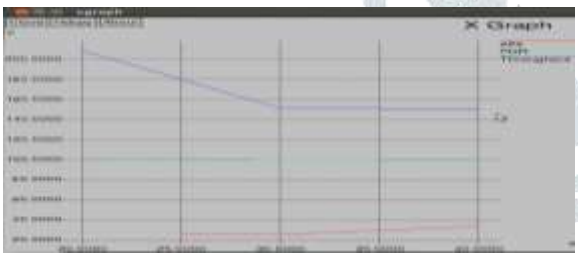
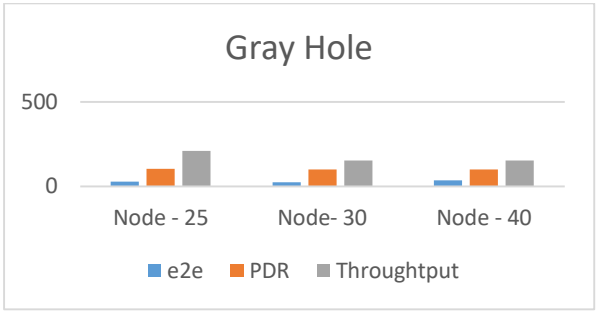


Fig5: Graph e2e, PDR, Throughput grayhole attack

Nodes	25	30	40
e2e	25.7744	24.7383	33.0175
PDR	101.68	99.84	99.58
Throughput	208.8	151.18	150.77

Table 1: Comparative result for Grayhole Attack



Bar Graph of comparative result of Gray hole attack

V. Conclusion

Since the mechanism for framing and refreshing trust is structured and implemented, it could be utilized for different purposes separated from route selection. The outcomes got from this paper are exceptionally intriguing for the advancement of other future works. Future work could be toward reenacting the convention in a larger network and to limit the overhead and delay. Additional mechanisms to battle control parcel dropping and flooding attacks and to build the fairness in the system are the conceivable regions for future research.

References:

[1] Valentina Timcenko, MirjanaStojanovic, SlavicaBostjancicRakas, "MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison," Proceedings of the 9th WSEAS International Conference on Applied Informatics And Communications, pp-271-276, 2009.

[2] Jing Deng, Richard Han, and Shivakant Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," University of Colorado, Department of Computer Science Technical Report CU-CS-951-03, pp-1-17.

[3] Seung Yi, Prasad Naldurg, Robin Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks," Dept. of Computer Science University of Illinois at Urbana-Champaign Urbana, IL 61801.

[4] V.Ramesh, Dr.P.Subbaiah, N. Koteswar Rao, M.Janardhana Raj, "Performance Comparison and Analysis of DSDV and AODV for MANET," (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 183-188.

[5] Abhishek Pandey, R.C. Tripathi, "A Survey on Wireless Sensor Networks Security," International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010.

[6] Akanksha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET," IJCST Vol. 1, Issue 2, December 2010.

[7] Preeti Sachan1, and Pabitra Mohan Khilar, "Security Attacks and Solutions in MANET," Proc. of Int. Conf. on Advances in Computer Engineering 2011.

[8] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[9] Yong Hao, Jin Tang, Yu Cheng, "Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs," IEEE Globecom 2011 proceedings, 2011.

[10] C.Gayathri, Dr.V.Kavitha, "Mitigation of Colluding Selective Forwarding Attack in WMNs using FADE," INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY VOLUME 3 ISSUE 1 –JANUARY 2015.