International Innovative Research Journal of Engineering and Technology

ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

Performance Analysys In Impact Of Trust Based Security Association And Mobility In Manet

K.Sivagurunathan[1], B.Vishnukumar[2]

[1]Assistant Professor,[2]Student,Department of Electronic and Communication Engineering,

Christ Institute of Technology,Pondicherry, India

[1]msg2sivaguru@gmail.com,[2]vishnukumarsjs@gmail.com

***Abstract* —** Trust models in the literature of MANET'S commonly postulate that packets have different security requisites. Afore a node forwards a packet, if the receiver trust level does not meet the packet's requisite level, then the recipient must perform certain security modality procedures, such as re-authentication. We present in this paper an analysis of the epidemic broadcast delay in such context. The network mobility and trust models presented in this paper are quite generic and sanction us to obtain the delay component induced only by the security modalities along a path. Numerical results obtained by simulations withal corroborate the precision of the analysis. In particular, we can observe from both simulations and analysis results that, for immensely colossal and sparsely connected networks, the delay caused by security modalities is diminutively minuscule compared to the total delay of a packet. This additionally betokens that parameters like network density and nodes velocity rather than any trust model parameter, have more impact on the overall delay.

Keywords — Depoissonization**,** Delay analysis, mobility, security association, trust.

I. INTRODUCTION

Past few years, have witnessed a rapid escalation in the field of mobile computing due to proliferation of inexpensive, widely available wireless contrivances. Thus, it has opened prodigious opportunity for researchers to work on Ad Hoc Networks. In a MANET, nodes within one another's wireless transmission range can communicate directly; however, nodes outside one another's range have to rely on some other nodes to relay messages. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host to make them reach the destination node.

MANET is one that converges as needed, not indispensably with any fortification from the subsisting infrastructure or any other kind of fine-tuned stations. This verbal expression can be formalized by defining an ad hoc network as an autonomous system of mobile hosts (MHs) (withal accommodating as routers) connected by wireless links, the amalgamation of which forms a communication network model in the form of an arbitrary communication graph. This is in contrast to the well-kenned single hop cellular network model that fortifies the desiderata of wireless communication by installing base stations (BSs) as access points. In these cellular networks, communications between two mobile nodes consummately rely on the wired backbone and the fine-tuned (BSs). In a MANET, no such infrastructure subsists and the network topology may dynamically vicissitude in an capricious manner since nodes are in liberty to move.

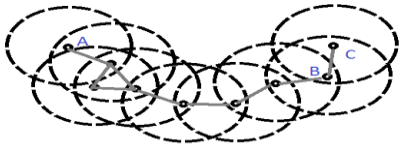

Fig 1 Data Flow in MANET

As for the mode of operation, ad hoc networks are fundamentally peer-to-peer multi-hop mobile wireless

networks where information packets are transmitted in a "store-and-forward" manner from a source to an arbitrary destination, via intermediate nodes as shown in Figure. As the MHs move, the resulting vicissitude in network topology must be made kenned to the other nodes so that archaic topology information can be either updated or abstracted.

SECURITY ISSUE IN MANET

Any system which is required to be secure might have weakness or vulnerabilities which would be targeted by an attacker.

A. Threat

Threat is the expedient through which the facility or intent of an agent to adversely affect an automated system, facility or operation can be manifested. All methods or things used to exploit an impotency in a system, operation or constitute threat agents. Examples of threats include assailants, astuteness accommodation etc.

B. Vulnerability

Vulnerability is any hardware or software imperfection that leaves an information system open for potential exploitation. The exploitation can be of sundry types, such as gaining unauthorized access to information or disrupt critical processing.

C. Attack

Attack is an endeavor to bypass the security controls on a computer system. The assailment may alter, relinquish, or gainsay data. It can privileges, inserting data mendaciously, modifying information, analyzing network traffic, obtaining illegitimate access to the system or disrupt network operation utilizing malignant software.

MODELS

We present in this section the network, mobility and trust models that the analysis is predicated on. The trust model additionally describes the communication protocol which is an epidemic broadcast, along with the conditions when two nodes need to perform an SA prior to forwarding a packet. These models provide the obligatory parameters as input to the mathematical model presented in Section IV that calculates the cessation-to-end delay.

A. Network models

Consequently, if the nodes move about arbitrarily, i.e. the nodes cull their destination points desultorily with uniform distribution over the space as in the desultory way point mobility model, then the relative angle between the directions of any two nodes taken arbitrarily and independently is withal uniformly distributed over $[0, 2\pi]$.

B. Mobility Models

We consider two mobility models: the arbitrary way point (RWP) and the desultory walk (RW). In each model, nodes move at a constant velocity v and to choose their direction independently of each other. With RW, nodes arbitrarily change directions every second. With RWP, each node arbitrarily culls a destination point on the square map then moves towards this point in a straight line. A node reiterates this process when reaching its destination. RW and RWP are commonly utilized in MANET simulations. These models are general enough to describe mobility in free space, since RW sanctions nodes to transmute direction within diminutive steps whereas RWP sanctions nodes to do so with more sizably voluminous steps.

C. Trust Model

In this trust model, each node monitors the trust value of its direct neighbours and former direct neighbours, i.e., the ones that used to be direct neighbours but are no longer. The trust value decays proportionally to the time the two nodes are out of each other's transmission area. Hence, a trust value in this model is a symmetrical, link-state metric, i.e., bound to a link between a dyad of node. If the link-state trust value with the receiver is deficient then the sender must trigger a trust instauration process, which may involve the authentication and the generation of an incipient session key. This process is kenned as security sodality or security handshake. We surmise that the process of trust instauration is equivalent to the process of an incipient trust establishment. After the security handshake, the link-state trust value is reset to and remains at 1 for as long as the two nodes are within the transmission range of each other.

MOBILITY ANALYSIS

In recent years, the prosperity of research in mobile ad hoc networks (MANETs) has led to the development of incipient applications in military and civilian domains such as wireless sensor networks and mobile contrivance comfort. For examples, frugal contrivances can be deployed in a truculent environment to monitor and report on enemy's activities, or authentication-capable controllers can be embedded in the equipment of each deployed unit to restrict their utilization to the sanctioned owner. We present in this

section the analysis of the average contact time and loss time between two nodes. We utilize simulations to validate the analytical results about mobility. The contact time and loss time are later utilized as inputs in the analysis of the terminus-to-end delay under security sodality procedures.

Related work

In it, the authors present architecture for managing SAs in MANETs. Each node has a state-machine to monitor the trustworthiness of the other nodes according to a customizable security policy (e.g., predicated on their identity, connection time, past comportment). Trust values decay with time and a security sodality is triggered if the trust level is low. Delay of epidemic broadcast has been extensively studied in the past. In one of the early work, it has been shown in it is possible to accurately soothsay the average delay, under some simple posits, from a Markov chain modeling the epidemic broadcast. Some of these results can additionally be obtained via nonlinear mundane differential .This method is later elongated in to include the density.

Variation of the infected population (i.e., nodes that have received the broadcast packet) during the epidemic broadcast. Other methods are kenned to provide an asymptotic result of the delay, especially when the number of nodes is high but the density is low and fine-tuned. In it, the authors utilize an Erdös-Rényi graph to study when a null graph eventually becomes connected under certain postulations on the connectivity rate of an arbitrary edge. In contrast, the authors of trace the delay from the probabilistic path (called journey) of a packet. This path-sagacious delay is broken into segments which i.i.d. desultory variables are representing the individual delays encountered by the packet on its path (e.g.: buffering delays, hop-to-hop transmission delays). The analysis presented in this paper follows this method, since breaking down the peregrination of a packet into segments sanctions us to introduce the segments of delay corresponding to the security handshakes. The rest of this paper is organized as follows. It describes the network, mobility and trust models on which the analysis is predicated. In it, we derive some mobility parameters that affect the proposed trust model. This result the accommodates as an input to the analysis of the asymptotic delay. Simulation results are presented below.

Simulation results

In this section, we present the performance evaluation on our technique utilizing extensive simulations conducted with the network simulator 2 (Ns allinone-2.35). We engendered desultory topologies with a maximum of 200 nodes over a rectangular field. The maximum transmission range of each node is 10m. The duration of the simulation is 11 s. Desultory waypoint model is utilized as the mobility model for each node. And we utilize simulations to verify the results obtained by analytical methods. We examine the total end-to-end delay and the delay induced by security handshakes alone.

Algorithm

A. Belief Propagation Algorithm

Belief propagation is known as sum product message passing is a message passing algorithm for interference on graphical model, such as Bayesian network and Markov random fields. The algorithm was first proposed by Judea Pearl in 1982. Belief propagation is commonly used in artificial intelligent and information theory. It include low density parity check code, turbo code and free energy approximation and satisfiability.

B. Adaptive Multipath Routing

In multi-hop network, the adaptive Quality of Service(AQos or AQR) protocol have been increasingly popular and have numerous application. One application in which it may be used in Mobile Ad hoc Network.

Step for algorithm:

1. Let h_n be the used next hop for the previous packet delivery from the source node n.

2. If β £ C_t then,

3. If $|C_t| > 1$ then,

4. Randomly choose a node X from $\{C_t - h_n\}$ as a next hop and send the packet to the X.

5. h_n ⟵ **X,** update the routing table of N.

6. else

7. Send the packet to h_n.

8. end if

9. else

10. A node Y can be randomly chosen from C_t as a next hop, and send the packet to the node Y.

11. h_n ⟵ Y, update the routing table of N.

12. end if

Here the two nodes are created and it can be given as X and Y. If the above following condition is satisfied then X is

ISSN NO: 2456-1983

assigned as h_n and if the condition is not satisfied then Y is assigned to h_n. And finally the process is end.

A. Performance Evaluation

Throughput Analysis

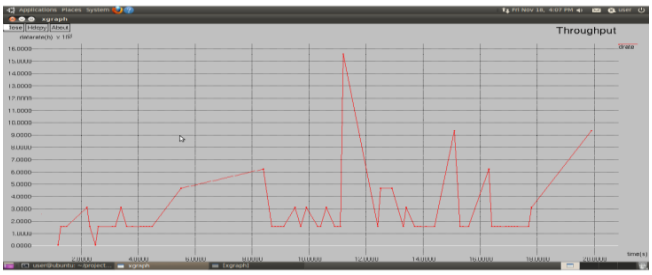

Fig 2 Throughput

Throughput = N/1000.

Where N is the number of node received successfully by all destinations.

The throughput of MANET is shown above, in which X-axis indicates the time in seconds and Y-axis indicates the data rate in bits. At the time of 11 seconds, there are 155 bits successfully delivered to the receiver.

Delay

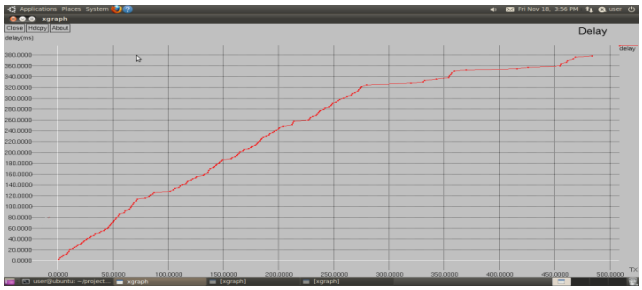

Fig 3 Delays - Belief Propagation Algorithm

Delay = N/R seconds.

Where,

N= Number of bits

R= Rate of transmission.

The delay graph of MANET is shown above, in which X-axis indicates transmitted bit and Y-axis indicates the delay in milliseconds. At the time of 180 milliseconds, there are 150 bits in queue to reach the receiver.

Drop

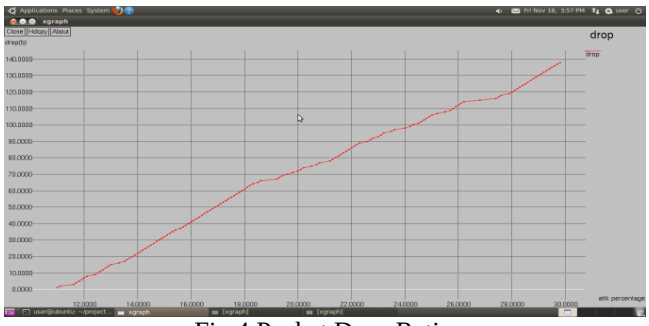

Fig 4 Packet Drop Ratio

Drop = Total number of packet – Received packet

The drop of MANET is shown above, in x-axis indicates the attacker percentage and in y-axis indicates drop in seconds. At the time of 40 seconds, there are 16 bits are dropped.

CONCLUSION AND FUTURE WORK

We present in this paper a mathematical model that sanctions for analyzing the delay of epidemic broadcast in a MANET where packets have different calibers of security requisite. The nodes have to perform a security sodality, such as re-authentication, if their trust level does not meet the packet's requisite. The network, mobility and trust models are quite generic. Utilizing this model, we obtain the asymptotic delay of the epidemic broadcast. In particular, we obtain the delay caused only by the security sodalities along a path. Simulation results additionally accede with the analytical results when varying different networking and mobility parameters such as density and node's velocity. We observe that for astronomically immense and sparsely connected networks, the delay caused by security sodalities contributes marginally to the overall delay of a packet. This shows that the parameters like network density and nodes' velocity play a more astronomically immense role in the delay than any security parameter. As a future work, amending network security with possible links and neighbor revelation, Minimizing loss due to link un-availability, Delay minimization.

ACKNOWLEDGMENTS

We thank our HOD **Dr.T.Thirumurugan**, Ph.D. (Department of Electronics and Communication Engineering) to help us for creating this paper with his sincere guidance and Technical Expertise in the field of

communication. The help of our guide **Mr.K.Sivagurunathan**, M.Tech, Department of ECE, Christ Institute of Technology is really immense and once again I thank her for her great motivation. I thank Christ Institute of Technology to provide me such a standard educational environment so that I am able to understand the minute concept in the field of Engineering and Technology.

REFERENCES

[1] S. Marsh, P. Briggs, K. El-Khatib, B. Esfandiari, and J. Stewart, "Defining and investigating device comfort," J. Inf. Process., vol. 19, pp. 231–252, 2011.

[2] M. Salmanianet al., "A modular security architecture for managing security associations in manets," in Proc. IEEE MILCOM, Nov. 2010.

[3] Elizabeth Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[4] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," J. Comput.Netw., vol. 51, pp. 2867–2891, July 2007.

[5] D. J. Klein, J. a. Hespanha, and U. Madhow, "A reaction-diffusion model for epidemic routing in sparsely connected manets," in Proc. IEEE INFOCOM,Mar. 2010.

[6] F. De Pellegrini, D.Miorandi, I. Carreras, and I. Chlamtac, "A graph-based model for disconnected ad hoc networks," in Proc. IEEE INFOCOM, May2007.

[7] P. Jacquet, B.Mans, and G. Rodolakis, "Broadcast delay of epidemic routing in intermittently connected networks," in Proc. IEEE ISIT, June 2009.

[8] P. Jacquet, B. Mans, and G. Rodolakis, "Information propagation speed in mobile and delay tolerant networks," IEEE Trans. Inf. Theory, vol. 56,no. 10, pp. 5001–5015, 2010.

[9] P. Jacquet and W. Szpankowski, "Analytical depoissonization and its applications," J. Theorical Comput. Sci., vol. 201, no. 1–2, pp. 1–62, 1998.

[10] D. Nguyen, T. Kunz, and L. Lamont, "Impact of mobility on trust decay rate," in Proc. IEEE WCNC, Apr. 2012.

BIOGRAPHY

Mr.K.Sivagurunathan is working as an Assistant Professor (Department of ECE) in CHRIST INSTITUTE OF TECHNOLOGY. He has done his UG degree in Electronics & Communication Engineering and PG degree in communication system. He has two years working experience as design engineer. He is interested in Ad-Hoc networks, Electro Magnetic wave theory, wave guides and antennas, signals and system.

Mr.B.Vishnukumar is a student who is pursuing B.Tech (Electronics and Communication Engineering) in CHRIST INSTITUTE OF TECHNOLOGY. He is interested in Ad-Hoc networks, Digital Circuit, Data communication Network, Data structure and Engineering Mathematics.