Volume 2, No. 6, June 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

Q-ROUTING AND INTRUSION DETECTION

D.B.Ojha[*1], Sharad Kumar Verma[2], Bhupendra kumar[2], Vinod Shukla[3] and Nitin Pandey[4]

*[1]Department of Mathematics, R.K.G.I.T., Ghaziabad, U.P., INDIA
ojhdb@yahoo.co.in[1]
[2]Department of Master of Computer Applications, M.I.E.T.,U.P., Meerut, INDIA
sharadverm@gmail.com [2]
[3]Department of Master of Computer Applications, I.I.M.T.,U.P., Meerut, INDIA
bhupe2002@gmail.com [3]
[4]Department of Information Technology, A.I.I.T., Noida, U.P., INDIA
npandyg@gmail.com[4]

Abstract: In this paper, we showed the procedure for solution of routing problem and intrusion detection. Our approach consist Q-routing and verification for authorization in MANET.

Keywords: Authentication,Intrusion Detection System (IDS),Mobile Ad hoc Network (MANET),Monitoring node, Security.

INTRODUCTION

All The protocols and systems which are meant to provide services can be the target of attacks such as Distributed Denial of Service (DDOS). Intrusion detection can be used as a second line of defense to protect network systems because once an intrusion is detected response can be put in place to minimize the damage or gather evidence for prosecution or launch counter offensives. Application concern of mobile ad hoc network include battlefields, emergency search, rescue missions, law enforcement and data acquisition in remote areas. A mobile ad-hoc network can be utilizable in classrooms and conferences where participants share information dynamically through their mobile computing devices. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

Intrusion detection techniques just like encryption and authentication systems which are the first line of defense have quite another aspect. As the system grows in complexity their weaknesses grow causing the network security problems to grow too. If an intrusion is detected then one can easily prevent intrusion or minimize the effects. There are several assumptions for developing IDS. In the first assumption, user operations and the programs are visible and in the Second assumption, normal and intrusive activities in a system behave differently. So, IDS should analyze system activities and ensure whether or not an intrusion has occurred. Intrusion detection can be classified based on audit data which are host or network based. A network-based IDS, receives packets from the network and analysis it. On the other hand, host-based IDS, analyses the events taken place in application programs or the operating systems. IDS can be divided into three groups based on detection techniques; anomaly detection system, misuse detection systems and specification based detection [(Brutch and Ko(2003), Rafsanjani, Movaghar and Koroupi(2008)]. In MANET, intrusion detection and response systems should be both distributed and cooperative in order to fulfill the needs of mobile ad hoc networks. For instance, in the architecture proposed by Y. Zhang, W. Lee and Y. Huang (2003), every node in the mobile ad hoc network participates in intrusion detection and response. Since every node cannot trust its neighboring nodes, it is responsible for detecting signs of intrusion locally and independently. However, neighboring nodes can collaboratively exchange messages in case of a suspicious situation or confirmed intrusion detection.

PRELIMINARIES

The detection scheme is based on the main operations of Ad hoc networks in link and network layers of Open Systems Interconnection (OSI) Reference Model.In link layer the cases of one-hop connectivity and frame transition, and in network layer, the cases of routing and data packet forwarding are considered [Zhou and Haas(1999), Komninos, Vergados and Douligeris(2007), Kong(2002)]. Data link layer protocols provide the connections between neighbouring nodes and will also provide the accuracy of the transmitted frames. As routing protocols exchange routing data between nodes, as a result, they would maintain routing states in each node. Based on routing states, data packets are transmitted by mediated nodes along an established route to the destination. The detection procedure, tried to detect the unauthorized nodes. This phase of our scheme is based on Komninos and et al.'s framework and use a non-interactive zero knowledge technique [Komninos, Vergados and Douligeris(2007)].

Rafsanjani and Movaghar(2008), a monitoring nodes selection method in the selected networks was presented in which detection scheme is proposed, for identifying unauthorized nodes.

Q -routing [Boyan & Littman (1994)] is an adaptive packet routing protocol for static networks based on the Q-learning works. It is essentially a version of the distributed Bellman-Ford algorithm. The algorithm allows a network to

continuously adapt to congestion or link failure by choosing routes that require the least delivery time. When a route becomes congested or fails, Q-routing learns to avoid that route and uses an alternate path. Due to its adaptive nature, we might expect that Q-routing would also work well in the mobile ad-hoc setting. Q-routing is a direct application of Watkins' Q learning [Watkins (1989)] to the packet routing problem. Each node in the network runs its own copy of the Q-routing algorithm. A node x faces the task of choosing the next hop for a packet destined for some receiver node d. Using Q-routing, it learns the expected delivery times to d for each possible next hop y, where each possible next hop y is a neighbor node connected to x by a network link. Formally, Q-routing keeps Q-tables Q_x for each node x and updates these tables at each time period t as follows:

$Q_t^x(d,y) = (1-\alpha)Q_{t-1}^x(d,y) + \alpha(b_t^x + \min_z Q_{t-1}^y(d,z))$, where $0 < \alpha < 1$ is parameter that controls the learning rate, and b_t is the time the current packet spent on the buffer or queue at node x before being sent off at time period t. Q-learning estimates the value or cost, V, associated with each state d, with $V = \min_z Q^x(d,z)$. Y. Chang, T. Ho and LP. Kaelbling,(2003) uses , the value of a state is the estimated time for delivery of a packet from the current node x to destination d via node z. Once the nodes have learned the values associated with each state-action pair, they simply execute a greedy policy to behave optimally. When a node receives a packet for destination d, it sends the packet to the neighbor y with the lowest estimated delivery time $Q^x(d,y)$. Adapting Q-routing to the mobile ad-hoc network routing domain is fairly straightforward. Neighbor nodes are defined as the nodes within transmission range. The main difference is that the neighbor nodes y may appear and disappear quite frequently due to node mobility. When a node y moves out of range, we set the estimated delivery time to d via y to ∞; i.e., $Q^x(d,y) = \infty$. When a node y moves into range, we optimistically set the estimated time to 0; i.e., $Q^x(d,y) = 0$. This optimistic bias encourages exploration. That is, node x will always try sending packets via a node y that has just come into range. If this action results in a high estimated delivery time, then node x will quickly revert to its original behavior since $Q^x(d,y)$ will quickly be updated to its true value. On the other hand, if this action results in a good delivery time, then node x will continue to send packets via node y.

RESULTS

Suppose D_{first} and D_{second} nodes are verified. When node N_1 enters the MANET, its authentication action is done by neighbouring nodes D_{first} and D_{second}. New routes will be built between nodes. As soon as nodes N_1 are verified as authorized nodes in the network, routing and transmitting packets would be done through them. There are several suitable protocols for authentication in the MANET which can be used. Of course, it is necessary to use protocols with low complexity and non-interactive which would not produce excessive computational overhead in the network. The interactive zero protocols are not suitable for the wireless environments because they exchange many messages and as a result the efficiency of the network decreases. The non-interactive zero knowledge protocols are proper for the MANET networks in such a way that the nodes do not need to exchange messages to verify their identities. For example, the node N_1 can prove its identity to the nodes D_{first} and D_{second} and guarantees that discrete logarithms of $w_1 = a^{d_1}$ and $w_2 = b^{d_2}$ are computed with a and b bases.

CALCULATIONS BEFORE ANALYSIS

Title Now the procedure followed by N_1, after convincing that discrete logarithms build linear equation to D_{first} and D_{second}:

Step 1: $gd_1 + hd_2 = V \pmod p$ where g,h,V are integers and p is a sufficiently large prime number, V is constant cost d_1, d_2 are intervals.

Step 2 : Calculate $w_3 = e^{d_3}$, $w_4 = j^{d_4}$ and solves $gd_3 + hd_4 = 0 \pmod p$.

Step 3: Message send by N_1 to D_{first} is $w_5 = a^{d_3}$.

Step 4: Message send by N_1 to D_{second} is $w_6 = b^{d_4}$.

Step 5: Message send with applying one –way Hash function by D_{first} and D_{second} to N_1 is $w_7 = H(a,b,g,h,V,w_1,w_2,w_5,w_6)$.

Step 6: After validation of w_5, w_6 by N_1, again message $w_8 = d_3 - w_7.d_1 \pmod p$ to D_{first} and $w_9 = d_4 - w_7.d_2 \pmod p$ to D_{second} .

Then after D_{first} and D_{second} calculate

$w_{10} = a^{w_8} w_1^{w_7}$, $w_{11} = a^{w_9} w_2^{w_7}$, $w_{12} = H(a,b,g,h,V,w_1,w_2,w_{10},w_{11})$, $gw_8 + hw_9$ and $w_7 V \pmod p$.

D_{first} and D_{second} ANALYSIS AFTER CALCULATIONS

1. If $w_{10} \neq w_5$ and $w_{11} \neq w_6 \Rightarrow w_{12} \neq w_7$. In another words, N_1 is not reliable.

2. If $gw_8 + hw_9 \neq w_7 V \pmod p \Rightarrow$ The identity of N_1 is not authorized.

CALCULATIONS

This article successfully showed the way how to make optimal decision for the routing problem and intrusion detection in MANET. Hence, it solves the problem in the concern of finding an optimal route and recognition of unauthorized intruder in a MANET.

REFERENCES

[1] L. Zhou and Z. J. Haas, Securing ad hoc networks, IEEE Network Magazine Special Issue on Network Security, 13(1999), 24-30.

[2] N. Komninos, D. Vergados and C. Douligeris , Detecting unauthorized and compromised nodes in mobile ad hoc networks, Elsevier Ad hoc network, 5(2007), 289-298.

[3] M. K. Rafsanjani and A. Movaghar, Identifying monitoring nodes with selection of Authorized nodes in mobile ad hoc networks, World Applied Science Journal, 4(2008), 444-449.

[4] J. Kong, Adaptive Security for Multi-layer Ad Hoc Networks, Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press, 2002.

[5] Y. Chang, T. Ho and LP. Kaelbling, Multi-agent learning in mobilized ad-hoc networks, AI Lab Memo, AIM-2003-025, 2003.

[6] Boyan, J., and Littman, M. L. 1994. Packet routing in dynamically changing networks: A reinforcement learning approach. In Advances in NIPS.

[7] Watkins, C. J. 1989. Learning with delayed rewards. Ph.D. Thesis, University of Cambridge.

[8] P. Brutch and C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, The Symposium on Applications and the Internet Workshop, 2003, 368-373.

[9] M. K. Rafsanjani, A. Movaghar and F. Koroupi, Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes, The Proceedings of World Academy of Science, Engineering and Technology, 2008, 351-355.

[10] Y. Zhang, W. Lee and Y. Huang, Intrusion detection techniques for mobile wireless network, Wireless Networks Journal, 9(2003), 545-556.

