COLLABORATIVE ANOMALY-BASED INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

SUNIL K. PARYANI

Information Technology Department,
Government Polytechnic, Ahmedabad

RAJESH PATEL

M. TECH STUDENT,
Nirma University, Ahmedabad

VIJAY UKANI

Associate Professor,
Nirma University, Ahmedabad

Abstract

Intrusion Prevention is first line of defense against attacks in MANET. Intrusion Detection and response presents a second line of defense. New vulnerabilities will continue to invent new attack methods so new technology such as MANET, we focus on developing effective detection approaches In this paper, we present an intrusion detection system for detection of malicious node in mobile ad hoc network. The technique is designed for detection of malicious nodes in a neighborhood in which each pair of nodes are within radio range of each other. Such a neighborhood of nodes is known as a clique. [1] This technique is aimed to reduce the computation and communication costs to select a monitor node and reduces the message passing between the nodes to detect a malicious node from the cluster hence there very less traffic and less chances of a collision.

Keywords: MANET; Collaborative; Intrusion detection system.

1. INTERODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. In recent years mobile ad hoc networks (MANETs) have received incredible attention because of their self configuration and self-maintenance capabilities. Fundamental vulnerability of MANETs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. Intrusion detection systems (IDS) on wireless networks are an open research topic. Intrusion detection is a technology for detecting hostile attacks against computer systems from both outside and inside. In terms of detection mechanism, the techniques for intrusion detection can be classified into two categories: signature-based detection and anomaly detection. Signature-based detection looks for evidences of malicious behavior matched against pre-defined descriptions of attacks or

signatures. Although signature-based detection is effective for detecting known attacks, it generally cannot detect the new attacks that are not predefined. Anomaly detection, on the other hand, builds the profile of normal behavior and attempts to identify the patterns or activities that deviate from the normal profile. Based on the concept of profiling normal behavior, a salient feature of anomaly detection is that it can detect unknown attacks. However, it may also cause significant number of false alarms since the model assumed to describe complete normal behavior may not be accurate, and obtaining such a model usually by machine learning is difficult. The research focus on anomaly detection is to find more effective and accurate methods. In this paper we propose an intrusion detection mechanism based on cooperative, anomaly based. The intrusion detection technique reduces the message passing between the nodes to detect a malicious node from the cluster hence there less traffic and less chances of a collision and the procedure for monitor node election is invoked and is aimed to reduce the computation and communication costs.

2. Motivations and Related Works

2.1. Motivation

Intrusion Prevention is first line of defense against attacks in MANET. Experience in security research in the wired environments has taught us that we need to deploy defense-in-depth or layered security mechanisms. So, many Intrusion Detection techniques have been developed in the wired networks, the vast differences in MANET need that we design new intrusion detection architectures and algorithms. Intrusion Detection and response presents a second line of defense. New vulnerabilities will continue to invent new attack methods so new technology such as MANET, we focus on developing effective detection approaches.

2.2. Related Works

In the following literature survey we found some of the proposed technique for intrusion detection. Manikopoulus and Ling [1] presented architecture for mobile ad-hoc network security where an intrusion detection system (IDS) runs on every node. This IDS collects local data from its host node and neighboring nodes within its communication range, processes raw data and periodically broadcasts to its neighborhood classifying normal or abnormal behavior based on processed data from its host and neighbor nodes[2]. Zhang et al. [3] developed architecture for intrusion detection which is distributed and cooperative. They also presented how anomaly detection could be done by using a classifier which is trained using normal data to predict what is normally the next event given the previous sequence of events. Deviation from the predicted event would mean that there is an intrusion. Nadkarni and Mishra [4] proposed intrusion detection scheme, based on the principle of misuse detection that can accurately match signatures of know attacks.

By N. Marchang, and R. Datta proposed new algorithm for intrusion detection in cluster. The algorithms use collaborative effort from a group of nodes for determining the malicious nodes by voting. Messages are passed between the nodes and depending on the messages received; these nodes determine suspected nodes (nodes that are suspected to be malicious). These suspected nodes (votes) are eventually sent to the monitor node (the initiator of the detection algorithm). At the monitor node, the suspected nodes that receive at least a minimum number of votes are finally detected as malicious nodes. Thus instead of giving the sole authority to a single node to decide about the maliciousness of another node, the algorithm works in such a way that a group of nodes together make this decision.[4] Deepak Kumar Sharma, Dr. S. K. Saxena, Ajay Kaushik, Vijay Tiwari [5] propose the algorithm uses collaborative efforts from a group of nodes for determining malicious nodes. For analyzing a particular node, the monitor node requests for the data packets from those two nodes that were to receive packets from the node under consideration. If even one of the two messages returned by the nodes matches with the actual data, the node is deemed as *secure*. Else, the node is marked as ‘suspicious’. The *monitor* node then uses the *secure* nodes to detect the malicious node(s) from the set of suspicious nodes. This method guarantees that no *secure* node is falsely accused to be malicious. The intrusion detection technique reduces the message passing between the nodes to detect a malicious node from the cluster hence there less traffic and less chances of a collision and the procedure for monitor node election is invoked and is aimed to reduce the computation and communication costs. The algorithms proposed in this paper are based on collaborative and monitor dependent intrusion detection system [4, 5]. As in [7], to run our algorithms, the network is divided into clusters, and the algorithms can be run in each cluster, with the cluster head as the monitor node. The proposed algorithms also take care of selection of stable monitor node based on A Weighted Clustering Algorithm [6] which find little or no mention in earlier works.

3. The Algorithm

A malicious node in this algorithm will modify the message before forwarding it or not forwarding the message at all. We have assumed that a malicious node will reveal these properties during its lifetime. This information can be used by the *clique*, and can also be passed to other *cliques*, so as to isolate the malicious nodes from themselves. The node that initiates the algorithm is called the *monitor* node. There exist several algorithms for grouping the nodes in a MANET into clusters [6] (cliques are known as 1-hop clusters) which are known as clustering algorithms. These algorithms specially assign a node in a cluster as the cluster-head. So, any clustering algorithm can first be applied to divide the network into clusters and then our algorithm can be used to those clusters with the cluster-heads as the *monitor* nodes. Also, because the *monitor* node has to carry out majority of the tasks in the detection process, its battery may get depleted faster than other members of the cluster. It can be taken care of by deploying clustering algorithms which elects new cluster-head from time to time depending upon node movement and battery power of node.

To present the algorithm we make the following assumptions:

(i) Assume that monitor node is not malicious.

(ii) The Intrusion Detection System that is capable of detecting at most k malicious nodes in a set (clique) of n nodes, where $n \geq 2k + 2$. [7]

The Algorithm has following steps.

Step 1. Find the neighbors of each node N nodes within its transmission range.

Step 2. Measure the mobility of node by M_N, as

$$M_N = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(X-X_{-1})^2+(Y_t-Y_{t-1})^2}$$

Where (X_t, Yt) and (X_{t1}, Y_{t1}) are the coordinates of the node N at time t and t_1, respectively

Step 3. Compute the cumulative time, P_N (how much battery power has been consumed) during which a node v acts as a Monitor node.

Step 4. Calculate the combined weight W_N for each node N, where

$$W_N = w_1 M_N + w_2 P_N$$

Where w_1 and w_2 are the weighing factors for the corresponding system parameters.

Step 5. Choose that node with the smallest W_N as the Monitor node.

Step 6: The monitor node M, sends a pair of messages to the remaining n-1 nodes, asking them to forward the messages to 2 other nodes.

Step 7: Each of the n-1 modes then forwards the messages to the intended nodes.

Step 8: The monitor node then analysis each of the remaining n-1 nodes, by sending a DATAREQUEST message.

Step 9: On receiving a DATA-REQUEST message, the 2 nodes then reply to the monitor with a DATAREPLY message.

Step 10: Upon inspecting each node, i.e. by taking back messages from all pair of *target nodes*, the monitor decides which nodes are malicious and which are not.

4. Conclusion and Future work

The algorithm uses collaborative efforts from a group of nodes for determining malicious nodes. For analyzing a particular node, the monitor node selected on the basis of combined effect of the mobility and battery power of

the nodes. Monitor node requests for the data packets from those two nodes that were to receive packets from the node under consideration. If even one of the two messages returned by the nodes matches with the actual data, the node is deemed as *secure*. Else, the node is marked as 'suspicious'. The *monitor* node then uses the *secure* nodes to detect the malicious nodes from the set of suspicious nodes. This method guarantees that no *secure* node is falsely accused to be malicious. Thus the algorithm detects the malicious nodes with high accuracy. Also, since each node has to forward messages to only 2 other nodes, hence this method greatly reduces congestion, and the probability of collision reduces further. However, for more than *k* malicious nodes in a set of *2k+2* nodes, the results may be unpredictable

In future Simulate and test the above presented algorithm and give statistical results to prove that the algorithm betters the throughput, since it lowers the number of messages passed considerably. Extend this algorithm to select the monitor node which takes into account its degree, transmission power also

References

[1] C. Manikopoulos, Li Ling: Architecture of the mobile adhoc network security (MANS) system, in: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, vol. 4, October 2003, pp. 31223127.
[2] Ningrinla Marchang a, Raja Datta b, N. Marchang, R. Datta: Collaborative techniques for intrusion detection in mobile ad-hoc networks, 2007
[3] Y. Zhang, W. Lee, Y. Huang : Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET.
[4] K. Nadkarni, A. Mishra: Intrusion detection in MANETs – the second wall of defense, in: Proceedings of the IEEE Industrial Electronics Society Conference'2003, Roanoke, Virginia, USA, November 2–6, 2003, pp. 1235–1239.
[5] N. Marchang, R. Datta: Collaborative techniques for intrusion detection in mobile ad-hoc networks, 2007
[6] M. Chatterjee, S.K. Das, D. Turgut, WCA: a weighted clustering algorithm for mobile ad hoc networks, Journal of Cluster Computing (Special Issue on Mobile Ad hoc Networks) 5 (2002) 193–204.
[7] O. Kachirski, R. Guha: Effective intrusion detection using multiple sensors in wireless ad hoc networks, in: Proceedings of 36th Annual Hawaii International Conference on System sciences (HICSS'03), January 2003,p.57.1