An Algorithm to Detect Bogus Nodes for a Cooperative Intrusion Detection Architecture in MANETs

Cao Trong Hieu*, Tran Thanh Dai, Choong Seon Hong*****
Dept. of Computer Engineering, Kyung Hee University
Email: hieuct@networking.khu.ac.kr, daitt@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract:
Wide applications because of their flexibilities and conveniences of Wireless Mobile Ad-hoc Networks (MANETs) also make them more interesting to adversaries. Currently, there is no applied architecture efficient enough to protect them against many types of attacks. Some preventive mechanisms are deployed to protect MANETs but they are not enough. Thus, MANETs need an Intrusion Detection System (IDS) as the second layer to detect intrusion of adversaries to response and diminish the damage. In this paper, we propose an algorithm for detecting bogus nodes when they attempt to intrude into network by attack routing protocol. In addition, we propose a procedure to find the most optimize path between two nodes when they want to communicate with each other. We also show that our algorithm is very easy to implement in current proposed architectures.

Keywords
Wireless Mobile Ad-hoc Networks (MANETs), Security, Intrusion Detection, Clustering, Attack on Routing Protocol

1. Introduction

Wireless Mobile Ad-hoc Networks (MANETs) currently become popular and are applied in many fields of daily life as well as military uses thank for their flexibility and adaptability. However, these networks change their topologies dynamically due to node mobility; lack concentration points where traffic can be analyzed for intrusions; utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communications channels that provide limited bandwidth and are subject to noise and intermittent connectivity [7][8][9].

To overcome the constraints, researchers have proposed a number of models and techniques not only for protection layer but also for detection and prevention layer. Among those kinds of techniques, distributed clustering is an efficient and realizable technique which is a framework for implementing security techniques. We propose to use clustering, which belong to data mining technique, can establish and maintain such a dynamic evolving hierarchy of intrusion detection components.

In this paper, we propose an algorithm for detecting bogus nodes when they attempt to intrude into network by attack routing protocol. In addition, we propose a procedure to find the most optimize path between two nodes when they want to communicate with each other.

The remainder of the paper is organized as follows. Section 2 briefly discusses some related work. Section 3 mentions about background study in this context, focusing on the hottest attack on MANETs. Section 4 describes the proposed algorithm and another simple procedure to find optimize path and make it available for implementation. Finally, in section 5, we discuss and summarize our results and future work.

This work was supported by MIC and ITRC project.

2. Related Works

Intrusion Detection currently is an interesting research field in the broad area of security. A lot of work has been done so far for Intrusion Detection in wired traditional networks [12,13,14,15]. Although many architectures and techniques are proposed, researchers did not give specific algorithms or procedures when solving problems to help their models reliable. Based on clustering technique which was first proposed by Zhang and Lee [17], D.Sterne in [5] has given an architecture inwhich the author solved almost drawbacks of a dynamic topology when implementing an IDS. But the same as almost related papers, the author has just explained some clues to detect bogus node in routing protocol and conclude that they can principle determine whether a node is an attacker. We have tried to find whether some papers gave and solved this shortcoming or not, but they considered it as definitely solved by default.

As we knew that attack in routing protocol is very hard to prevent, especially in wireless environment where the traffic can be easily eavesdrop. Once this kind of attack was done, attackers can do everything. Yi-an Huang in [6] was also proved his Cooperative IDS in anomaly detection and done his work using clustering technique, suggesting a series of protocol in this field based on AODV (Ad hoc On-demand Distance Vector) [18][19][20] which we also proposed in our work, but his system still did not detect and prevent this kind of attack.

A lot of works have been done in order to find a comprehensive model for IDS using clustering technique [1-6], but they have the same drawback, that is only showed their techniques in general that make them difficult to implement.

3. Background

3.1. Attack on MANETs

From the point of view of intrusion detection and response, we need to observe and analyze the anomalies due to both the consequence and technique of an attack. While the consequence gives evidence that an attack has succeeded or is unfolding, the technique can often help identify the attack type and even the identity of the attacker. Attacks in MANET can be categorized according to their consequences as the following:

1. Black hole: All traffics are redirected to a specific node, which may not forward any traffic at all.
2. Routing Loop: A loop is introduced in a route path.
3. Selfishness: A node is not serving as a relay to other nodes.
4. Denial-of-Service: A node is prevented from receiving and sending data packets to its destinations.
5. Network Partition: A connected network is partitioned into k (k ≥ 2) sub-networks where nodes in different sub-networks cannot communicate even though a route between them actually does exist.
6. Sleep Deprivation: A node is forced to exhaust its battery power.

Some of the common attacking techniques are:

1. Cache Poisoning: Information stored in routing tables is either modified and deleted or injected with false information.
2. Fabricated Route Messages: Route messages (route requests, route replies, route errors, etc.) with malicious contents are injected into the network. Specific methods include:
(a) False Source Route: An incorrect route is advertised into the network, e.g., setting the route length to be 1 regardless where the destination is.
(b) Maximum Sequence: Modify the sequence field in control messages to the maximal allowed value. Due to some implementation issues, a few protocol implementations cannot effectively detect and purge these "polluted" messages timely so that they can invalidate all legitimate messages with a sequence number falling into normal ranges for a fairly long time.
In this paper, we will concentrate on solving this kind of attack, prevent and exclude intruders at any time they attempt to break routing mechanism.
3. Spoofing: Inject data or control packets with modified source addresses.
4. Packet dropping: A node drops data packets (conditionally or randomly) that it is supposed to forward.
5. Rushing: This can be used to improve Fabricated Route Messages. In several routing protocols, some route message types have the property that only the message that arrives first is accepted by a recipient. The attacker simply disseminates a malicious control message quickly to block legitimate messages that arrive later.
6. Wormhole: A tunnel is created between two nodes that can be utilized to secretly transmit packets.
7. Malicious Flooding: Deliver unusually large amount of data or control packets to the whole network or some target nodes.

3.2. Clustering technique

Clustering is the method of grouping objects into meaningful subclasses so that the members from the same cluster are quite similar, and the members from different clusters are quite different from each other. Therefore, clustering methods can be useful for classifying network data and detecting intrusions [1-5].

Clustering analysis, which belongs to data mining technique, can classify unlabeled data. this technique can detect new and unknown types of intrusions with higher detection rate and lower false alarm rate compare with other techniques.

In this technique, nodes will communicate intrusion detection information most often with other nodes that are their parents or children in the hierarchy.

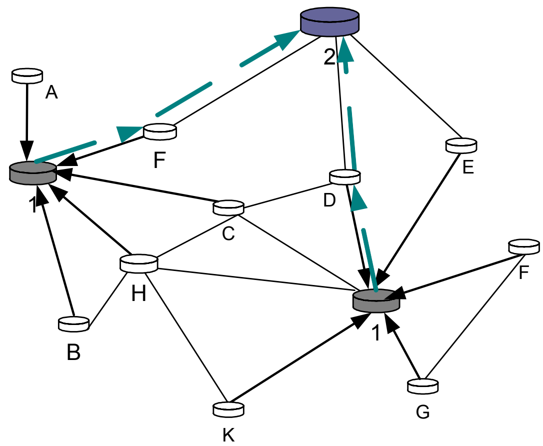


Figure 1: Simple clustering topology

Nodes annotated with a "1" are the representatives of first level clusters, mean leaf nodes in their cluster report to them (shown by arrows) "1"s in a cluster also report to their second lever representatives, also "2"s report to the third level.

To avoid having a single representative node at the top of the hierarchy that is a potential single point of failure, one or more members of the highest level cluster should be designated as backup representatives.

Cluster-head selection occurs at many levers (from peer nodes to level 1, level2, and so on)

Nodes at the lower level have main responsible for detection, data acquisition, after that intrusion detection data of all forms including alerts will generally flow upward and will be consolidated, correlated, and summarized incrementally as it flows upward.

A small collection of nodes at the uppermost level the hierarchy will serve as security management nodes that may possess an integrated view of the overall cyber security of the network. They also make decision to respond with attacks and transfer from top to bottom.

4. Proposed Algorithm

In the proposed cooperative intrusion detection architecture using clustering technique [5], the authors show their solution to detect attack on MANETs routing protocol, but they did not give any algorithm to prove that their technique can detect and exclude bogus nodes. Further more, they also do not give procedure with specific criteria to find a shortest (the most optimize) path.

In this paper, we do both two jobs: the first one is propose procedure to find a shortest (the most optimize) path using two most important criteria, signal strength and bandwidth. The second one is given algorithm to identify and exclude bogus nodes.

To implement our proposal, some pre-conditions are established.

We use the clustering technique to maintain the dynamic hierarchy and can automatic reconfigure follow nodes' mobility. We also use AODV (Ad hoc On-demand Distance Vector) as routing protocol in our proposal.

4.1 Shortest (the most optimize) Path Procedure

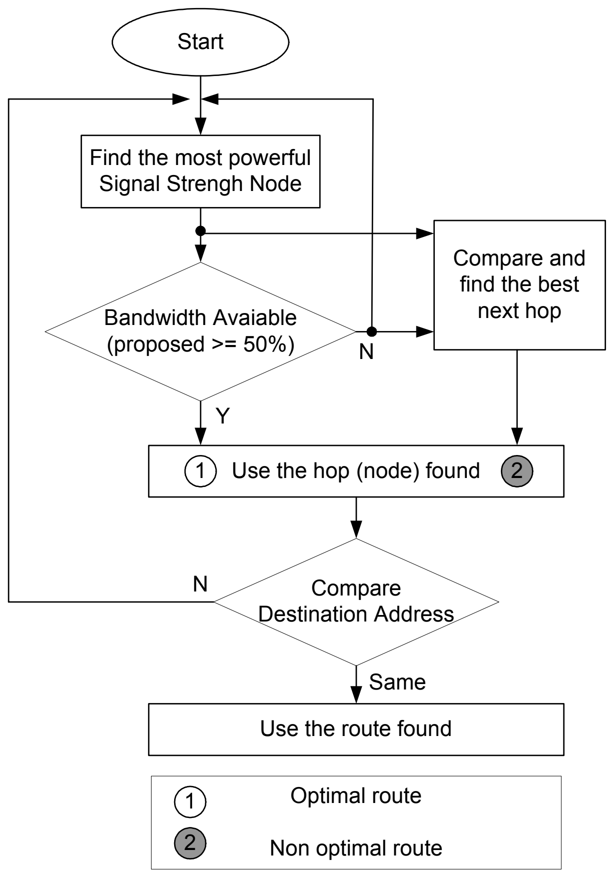


Figure 2: The Most Optimize Path Procedure

There are many criteria to decide a node has ability and capacity to become an intermediate node in a route. In such a dynamic topology like MANETs, it is very difficult to find a completely good routing protocol which can automatically reform and maintain connection. The most two important criteria we use in our procedure are Signal strength and Bandwidth because they guarantee for a stable and high speed connection. When a node wants to communicate with another one, the following steps are processed:

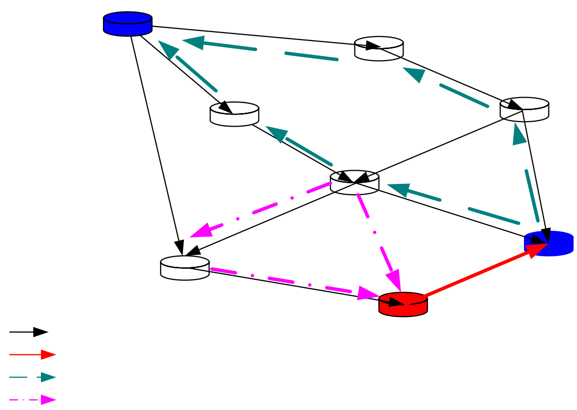
Step1: The source node floods RREQS packets with destination address to its neighbors and finds the node with the most powerful signal strength.

Step2: Estimate the available bandwidth of this node, if its free bandwidth ≥ 50%
Choose this node as a next hop
Else, compare with others lower signal strength nodes to find the most optimistic node
End if

Step3: Compare Destination Address
If Destination reached, stop
Else, repeat Step 2

Step4: Choose the route
Finish
In step2, the available bandwidth is assigned ≥ 50%, this value can be adjusted to suit requirement in a specific network. If a node with highest signal strength and enough bandwidth found in each hop, it means the optimal route was found. If not, we also can find the best route at final part step2. Based on the requirements of network, we can add other criteria such as proximity, resistance to compromise, accessibility, processing power, storage capacity, energy remaining, etc. to the procedure.

4.2. Identify and exclude Bogus Nodes



Initial
RREQS = 1, RREPD = 0
Flood RREQS in the network topology
for each time RREQS reaches node i
do RREQi = RREQi + 1
Nhop i = RREQi
compare destination address
if destination found
do Co-revise Procedure
{
for each route found from S to D
send RREPD back through other routes different from route of the first reach RREQ packet
RREPDj = Nhop j - j
compare (RREQj , RREPj) index
if RREPj index determined by neighbor nodes ≠ RREQj index
trigger an alarm
}
exclude j out of connection
Finish

To avoid bogus nodes modify again the RREP packet before send it back to the same route, the destination node will send RREP packets through other routes. By this way, Co-revise

Procedure can completely identify intruders. At least two neighbors of bogus node will ensure that node X is intruder by themselves, after compare RREQ index that X modified and sent with its real RREQ. How to do this?

Assume X is attacker and it is trying to access to the route between A and D. Normally, RREQA =1, A floods its request to find optimal route to D. In the Figure3, RREQB,H,F = 2 because they are neighbors of A, and RREQG,E = 3 and so on until the RREQ reaches D. If X is a legal node and it is in network topology, RREQX must be 3, but it modified this index, suppose RREQX = 2, and sends to D. Without our proposed algorithm, D will "think" the route include X is optimal, and choose this route. But now D can use proposed algorithm above, send back RREP to other route, like D,E,H,A and D,G,F,A . After that, B and E can themselves calculate the real RREQ index of X, and find it have to logical = 3. Also, if RREQX = 2, it means X have to a neighbor of A like B,E,F, but A can itself determine C is not a neighbor because A can not directly communicate with X. In briefly, the algorithm can definitely detect X is intruder, trigger an alarm and exclude X out of network.

5. Discussion

Our proposal approach in this paper bases on dynamic topology maintained by clustering technique and uses AODV as the routing protocol, inherits the achievements of previous researchers and improve shortcomings in their proposals. The algorithm can be easily applied when we insert additional fields Sequence Number into routing table. The simplicity of our algorithm so that does not require a considerable amount of computational resource, even there are a large number of nodes in a selected route. Each time the algorithm found the next hop, the process return to the initial point at step1 and do the same job of a loop. Consequently, the number of nodes in route are the exactly times needed to process, and the complexity in each step is trivial.

However, the simulation is needed to illustrate the light-weigh and strongly prove the result of this algorithm. Also, we will continue apply this algorithm in experiments and find out the best fit for each specific system.

References

[1] Portnoy, L. Eskin, E. Stolfo, S. J. Intrusion detection with unlabeled data using clustering. In: Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001). Philadelphia, ACM Press, 2001 (11).

[2] Xiangyang, Li. Clustering and Classification Algorithm for Computer Intrusion Detection [PhD.], Arizona State University, December 2001.

[3] Guan, Y. Ghorbani, A. Belacel, N. Y-means: A clustering method for intrusion detection. In: Proceedings of Canadian Conference on Electrical and Computer Engineering, Canada, 2003,1083-1086.

[4] Stefano Basagni, "Distributed Clustering in Ad Hoc Networks," Proceedings of the 1999 Intl. Symp. On Parallel Architectures, Algorithms and Networks (I-SPAN '99), Freemantle, Australia, 1999.

[5]. D.Sterne, A General Cooperative Intrusion Detection Architecture for MANETs, Proceeding of the Third IEEE International Workshop on Information Assurance (IWIA'05), 0-7695-2317-X05 IEEE

[6] Yi-an Huang, Wenke Lee A Cooperative Intrusion Detection System for Ad Hoc Networks 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03) October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA

[7] Vesa Karpijoki, "Security in Ad Hoc Networks" http://citeseer.nj.nec.com/karpijoki01security.html

[8] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Ad Hoc Network," IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.

[9] Konrad Wrona, "Distributed Security: Ad Hoc Networks & Beyond" PAMPAS Workshop, Sept. 16/17 2002, London

[10] A framework of cooperating Intrusion Detection based on Clustering analysis and expert system, De-gang Yang, InforSecu04, November 14-16, 2004, Pudong Shanghai, China, Copyright 2004 ACM ISBN: 1-58113-955-1

[11] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan. A cluster-based approach for routing in dynamic networks. ACM SIGCOMM Computer Communication Review, 27(2):49{64, 1997}.

[12] M.-Y. Huang, R. J. Jasper, and T. M. Wicks, A large scale distributed intrusion detection framework based on attack strategy analysis, Computer Networks, 31 (1999), pp. 2465–2475.

[13] Jake Ryan, Meng-Jang Lin, Risto Milikkulainen, Intrusion Detection with Neural Networks, Advances in Neural Information Processing Systems 10 (Proceedings of NIPS'97, Denver, CO), MIT Press, 1998.

[14] K. Ilgun, R. A. Kemmerer, and P. Porras, State transition analysis: A rule-based intrusion detection approach, IEEE Trans on Software Engineering, 21 (1995), pp. 181–199.

[15] P. A. Porras and P. G. Neumann, Emerald: Event monitoring enabling responses to anomalous live disturbances, in Proc of 20th NIST-NCSC Nat'l Info Systems Security Conf, 1997, pp. 353–365.

[16] O. Kachirski, R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), January 06 - 09, 2003.

[17] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, August 2000.

[18] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing." IETF RFC 3561.

[19] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, and Karl Levitt, "A Specification-Based Intrusion Detection System For AODV," Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), October 2003.

[20] C. E. Perkins and E. M. Royer. The ad hoc on-demand distance-vector protocol. In C. E. Perkins, editor, Ad Hoc Networking. Addison-Wesley, 2000.