Misbehavior Detection in Wireless Mesh Networks

Md. Abdul Hamid, Md. Shariful Islam, and Choong Seon Hong
Networking Lab, Department of Computer Engineering, Kyung Hee University,
1 Seocheon, Giheung, Youngin, Gyeonggi, 449-701, Korea
{hamid, sharif}@networking.khu.ac.kr and cshong@khu.ac.kr

Abstract **— In this paper we propose a detection technique to identify misbehaving client in wireless mesh networks. The technique is devised based on the communication history for two communicating clients through a common set of routers. Individual trust relationship is calculated for both the clients with their common routers. Then a correlation value for each client is found and compared with a predefined threshold to determine whether a client is spurious or not. We evaluate the performance of the proposed detection technique through simulation and results show that the detection efficiency is better with small number of misbehaving clients.**

Keywords **— WMN Security, Misbehavior Detection, Correlation.**

1. Introduction

Wireless networks provide unprecedented freedom and mobility for a growing number of laptop and PDA users who no longer need wires to stay connected with their workplace and the Internet. Ironically, the very devices that provide wireless service to these clients need lots of wiring themselves to connect to private networks and the Internet. This wiring is expensive to install and change, and deployment must be carefully planned and timed to minimize disruption to normal business operations. With all the work involved, it should not be surprising that wiring can be the most expensive part of a "wireless" network. Indeed, the many obstacles associated with wiring are now preventing or delaying the deployment of wireless applications that could deliver a real competitive advantage or a high return on investment—or both. Certainly a viable alternative to all those wires is the wireless mesh network. The wireless mesh offers a breakthrough approach that enables making the leap from localized Hot Spots to fully wireless Hot Zones with building-wide or campus-wide coverage and even Hot Regions that span an entire metropolitan area. Unlike basic Wi-Fi that simply untethers the client; the wireless mesh untethers the network itself giving IT departments, network architects and systems integrators unprecedented freedom and flexibility to build out networks in record time with high performance and without the expensive cabling.

The most important thing to remember is that the mesh topology is very different from the hierarchical hub and spoke topology presently used in most enterprise and service provider networks (Fig. 1). What distinguishes the wireless mesh network (WMN) from other topologies is the generous number of interconnections among neighboring nodes throughout the network [8]. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. Although this improves overall performance and resiliency, it is the sheer number of these interconnections that makes implementing a mesh with wires either impractical or impossible. The self-configuring and self-tuning abilities help give the mesh its third advantage as a self-healing network. The multiple redundant paths add robust resiliency and, when properly arranged, eliminate single points of failure and potential bottlenecks within the mesh.

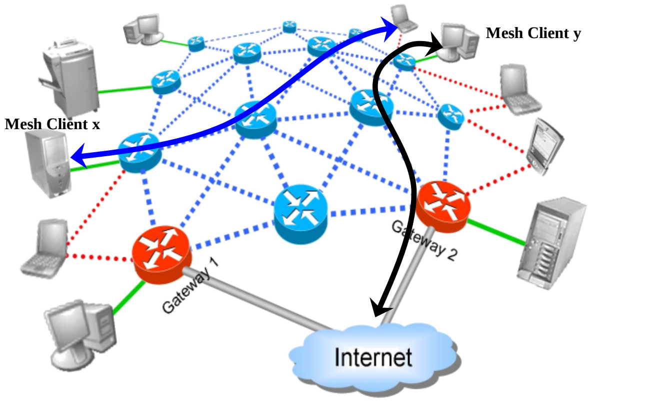


Figure 1. Client-client data flow and Client-Internet data flow through mesh routers and/or gateway in wireless mesh networks.

However, the network is compounded by the fact that mesh clients (MCs) are dynamic in the sense they may join and leave the network at any time they want. For example, Fig. 1 shows two communicating clients *x* and *y* via a set of mesh routers (MRs), after some period, a client may leave the network and join in other period and communicate via other set of routers. This will result in the possibility of some clients to be misbehaving or spurious and may impair the network from achieving its desired goal. Hence, without a convincing security solution, WMNs will not be able to succeed due to lack of incentives by customers to subscribe to reliable services [7]. As a consequence, new security schemes ranging from encryption algorithms to security key distribution, secure MAC and routing protocols, intrusion detection, and security monitoring need to be developed. A framework of intrusion detection in ad hoc networks is proposed in [9]. However, how to design and implement a practical security monitoring system, including cross-layer secure network protocols and

"This research was supported by the MIC under the ITRC support program supervised by the IITA" (IITA-2007-(C1090-0701-0016)).

Dr. C. S. Hong is the corresponding author.

various intrusion detection algorithms, is a challenging research topic. In this paper, we devise an efficient technique to detect misbehavior and identify the exact client to defend the network being flawed.

The rest of this paper is organized as follows. We describe related works in Section 2. Section 3 describes our approach and simulation results in details and Section 5 concludes this paper.

2. Related Works

Security is always a critical step to deploy and manage WMNs but security in multi-hop WMN has been given a little attention in the research community. In [1], the authors have identified the network operations that need to be secured in WMN are detecting corrupted router, securing routing protocol and enforcing a fairness metric. They also referred to adapt existing solutions proposed for ad-hoc network security. However, they ignored the class of attacks and malicious behavior of mesh clients. Zhang et al. in [2] have come up with an attack resilient security architecture for multi-hop WMNs. They have modeled WMN architecture as credit card based e-commerce system and showed that a mesh client needs not to be bound to a specific WMN operator, can get ubiquitous network access by a universal pass issued by a third-party broker. They used identity-based public key cryptosystem for authentication and key agreement between mesh clients and routers. Ref. [3] and [4] addressed the issue of privacy in WMN. But, both focused on the traffic privacy by proposing some anonymous routing algorithm. They have ignored how to deal with identity privacy and not mentioned how authentication and key agreement are performed between mesh nodes. Authors in [5] have shown an effective way to modeling a node-capture attack in multi-hop WMN by formulating it as an integer-linear programming minimization problem. They claim that privacy-preserving key establishment protocols can help to prevent minimum cost node capture attack. In [6], the authors have proposed an active cache based mechanism to defend DoS attack caused by flooding a large volume of traffic in the network by malicious intruders. They used most frequently used caching mechanism to identity flooding and raise an early alert to defend the attack. Authors in [10] considers the problem of joint routing, scheduling and transmission power assignment in multi-hop wireless mesh networks with unknown traffic. The objective is to minimize the maximum of the total transmission power in the network over all traffic matrices in a given polytope

To enhance security of WMNs, two strategies need to be adopted [7]: (a) either to embed security mechanism into network protocols such as secure routing and MAC protocols or, (b) to develop security monitoring and response systems to detect attacks, monitor service disruption, and respond quickly to attacks. Our work focuses on the misbehaving mesh clients that are detected based on the trust relationship with mesh routers through which they communicate. The detection algorithm runs in every mesh router in a cooperative manner and the decision is passed to client from the router that serves this particular client.

3. Detection Technique

We develop a preventive solution to deal with the colluding actions taken by the malicious intruders, i.e., misbehaving mesh clients. Fig. 2 shows the communication scenario between two MC, *x* and *y* via a common set of routers. Common set is chosen based on the close relationship with the two communicating clients. For example, all the past messages between client *x* and *y* traverse through this set of routers and/or both clients have individual communications with those routers and therefore they have an existing trust history with the routers. Based on this trust relationship, an algorithm is developed to calculate the correlation between client *x* and *y* and a decision whether client *y* is misbehaving or not is sent to client *x* at the time client *x* wants to communicate with *y*.

Suppose $M = \{MR_1, MR_2, MR_3, \ldots, MR_m\}$ is a common set of routers through which clients MC_x and MC_y exchange messages. We define two set trust values $T_x = \{t_1, t_2, t_3, \ldots, t_m\}$ and $T_y = \{t_1, t_2, t_3, \ldots, \mathrm{t_m}\}$ for the two clients MC_x and MC_y, respectively. Then, individual trust between MC_x and its common communicating set M is evaluated as $t_1 = (S_{xMR1} - F_{xMR1}) / (S_{xMR1} + F_{xMR1})$, $t_2 = (S_{xMR2} - F_{xMR2}) / (S_{xMR2} + F_{xMR2})$,…, $t_m = (S_{xMRm} - F_{xMRm}) / (S_{xMRm} + F_{xMRm})$. Similarly, individual trust between MC_y and M is evaluated as $t_1 = (S_{yMR1} - F_{yMR1}) / (S_{yMR1} + F_{yMR1})$, $t_2 = (S_{yMR2} - F_{yMR2}) / (S_{yMR2} + F_{yMR2})$,…, $t_m = (S_{yMRm} - F_{yMRm}) / (S_{yMRm} + F_{yMRm})$. Here, *S* and *F* denote the individual rate of legitimate and malicious messages respectively while communicating with the common set *M*.

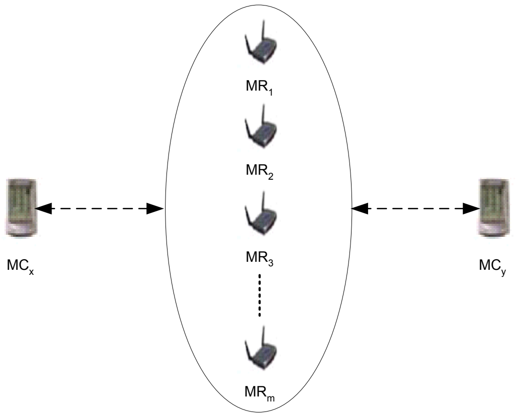


Figure 2. A snapshot between two communicating mesh clients MC_x and MC_y via common set of mesh routers MR_1, MR_2, …, MR_m.

Then we calculate the correlation ρ according to (1) as

$$\rho(T_x, T_y) = cov(T_x, T_y) / \sigma_{T_x} \sigma_{T_y} \tag{1}$$

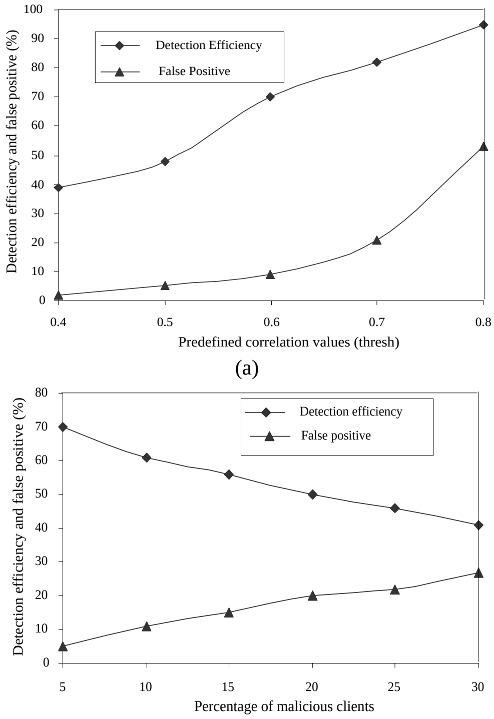
where σ_{T_x}, σ_{T_y} are the standard deviations of client x and y, respectively. Based on this correlation value, a decision is made whether a client is misbehaving or not.

Misbehavior Detection Algorithm (MDA) depicts the detection procedure that runs in each mesh router. Each router has to compute $O(N^2)$ operations to cooperatively calculate the correlation for the communicating mesh clients. However, the number of operations reduces to O(1) as it uses the previously calculated value to pass the decision to a legitimate client.

Misbehavior Detection Algorithm

Input: Past communication history of mesh client *x* and *y* and common set of routers {*M*}.
Output: Decision whether client *y* is misbehaving or not.
Procedure:

1. Calculate the past trust values T_x and T_y.
2. Divide the common set {*M*} and trust values T_x and T_y into *g* groups ($g \geq 1$) as $\{\{T_{x1}\},\{T_{x2}\},\ldots, \{T_{xg}\}\}$and $\{\{T_{y1}\},\{T_{y2}\},\ldots,\{T_{yg}\}\}$.
3. Arrange the trust values according to groups as $\{\{T_{x1},T_{y1}\},\{T_{x2},T_{y2}\},\ldots\{T_{xg},T_{yg}\}$ and calculate the correlation according to Eq. 1.
4. Calculate the average correlation $\rho_{avg} = \sum_{i=1}^{g} \rho_i / g$.
5. Compare the correlation with a predefined threshold *thresh*, if $\rho_{avg} \leq$ *thresh*, return *true*, else return *false.*



(a)

(b)

Figure 3. Performance evaluation. (a) Detection efficiency ε and False Positive Υ with different threshold values. (b) ε and Υ with different percentage of misbehaving clients (*thresh* = 6.5).

Simulation Results: We evaluate the performance of algorithm MDA through simulations. We consider networks of 100 mesh routers uniformly located in a square area and under each router there are 8 mesh clients. By executing MDA algorithm, before communicating with a client *y*, a legitimate client *x* gets the decision whether *y* is legitimate or malicious based on the previous communication history with the set of routers common to both *x* and *y*. We set legitimate and malicious message ratio as 75:25 for normal client, whereas a misbehaving client always sends malicious messages.

Detection Efficiency: Let *u* and *v* denote the number of malicious client detected and total number of malicious clients, respectively. Then, the detection efficiency ε is defined as $\varepsilon = u / v$. And let *p* denote the number of legitimate clients detected as malicious ones and *q* denote the total number of clients. Then, false positive rate Υ is defined as $\Upsilon = p / q$. Fig. 3 shows the simulation results. Optimal threshold value (i.e., detection efficiency is high with minimum false positive) may be found between 0.6 and 0.65 from Fig. 3a. 80% efficiency may be achieved under threshold value 0.65 keeping the false positive rate around 10% as shown in Fig. 3a. Fig. 3b shows the efficiency and false positive rate under optimal threshold 0.65 and we conclude that our algorithm performs better when the percentage of misbehaving clients is smaller. So, the algorithm has its limitation as the detection efficiency gets confined by the number of misbehaving clients.

4. Conclusion

In this paper, we have investigated how to mitigate the colluding actions taken by the mesh clients in multi-hop wireless mesh networks by exploiting the existing communication history that two communicating clients build with their common set of routers. It is shown that our detection technique performs better with small number of misbehaving clients. As a future work, we plan to further improve this limitation by solving the problem of reducing the false positive rate while increasing the detection efficiency. We also plan to develop the detection technique for mesh routers.

References

[1] N.B.Salem, H.P. Hubaux, “Securing wireless mesh networks,” IEEE Wireless Communications, April, 2006. pp. 50-55.

[2] Y. Zhang, Y. Fang, “ARSA: An attack resilient security architecture for multihop wireless mesh network,” IEEE Journal on Selected Areas in Communications, vol.24. no.10, October, 2006. pp. 1916-1928.

[3] X.Wu , N. Li, “Achieving privacy in Mesh Networks,” in proceedings of SASN’06, pp- 13-22, Oct. 30, 2006.

[4] W. Taojun, X. Yuan and Y.Cui, “Preserving traffic privacy in Wireless Mesh Networks,” in prod of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM’06).

[5] P. Tague, R.Poovendran “Modeling Node Capture Attacks in Multi-hop Wireless Networks,” Ad Hoc Networks, vol. 5 issue 6, August 2007, pp. 801- 814.

[6] Santhanam, L., Nandiraju, D., Nandiraju N., Agrawal D.P., “Active Cache Based Defense against DoS Attacks in Wireless Mesh Network,” 2nd International Symposium on Wireless Pervasive Computing, ISWPC '07, 5-7 Feb. 2007, pp. 419-424.

[7] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A Survey,” Computer Networks (Elsevier), 47(4), 2005, pp. 445-487.

[8] Intel Inc., Multi-Hop Mesh Networks—a new kind of Wi-Fi network.

[9] Y. Zhang, W. Lee, “Intrusion detection in wireless ad hoc networks,” ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), 2000, pp. 275– 283.

[10] A. Kashyap, S. Sengupta, R. Bhatia and M. Kodialam, “Two-Phase Routing, Scheduling and Power Control for Wireless Mesh Networks with Variable Traffic,” ACM SIGMETRICS’07, June 12–16, 2007, San Diego, California, USA, pp. 85-96.