Multiple Attributes Based Spoofing Detection Using an Improved Clustering Algorithm in Mobile Edge Network

Shida Xia*†, Na Li*†, Xiaofeng, Tao*†, and Chao Fang‡

* National Engineering Lab for Mobile Network Technologies, Beijing, 100876, China.
†Beijing University of Posts and Telecommunications Research Institute, Shenzhen, 518000, China.
‡Faculty of Information Technology, Beijing University of Technology, Beijing, 100876, China.

***Abstract*—Information centric network (ICN) based Mobile Edge Computing (MEC) network has drawn growing attentions in recent years. The distributed network architecture brings new security problems, especially the identity security problem. Because of the cloud platform deployed on the edge of the MEC network, multiple channel attributes can be easily obtained and processed. Thus this paper proposes a multiple channel attributes based spoofing detection mechanism. To further reduce the complexity, we also propose an improved clustering algorithm. The simulation results indicate that the proposed spoofing detection method can provide near-optimal performance with extremely low complexity.**

***Index Terms*—Mobile Edge Computing, multiple attributes, spoofing detection, cluster algorithm.**

I. Introduction

In past decade, Mobile Edge Computing (MEC) network get more attention as network traffic convert to large scale and multimedia. Security problems become particularly important due to its edge network architecture, in which the traditional security architecture have been inefficient or even unsuitable [1]. Identity authentication problem is the main security issues in decentralized cloud computing architecture, which would induce spoofing attack, floor attacks, and authority attacks and etc [2]. Spoofing attacks is the most common authentication attacks which can cause great harm for MEC network, such as sensitive information disclosure, modifications.

At present, there are few research on tackling spoofing attack or intrusion detection in MEC network. However, it is also meaningful to reference the spoofing detection mechanism of the cloud computing networks and wireless networks. In [3], the signature based detection is proposed that seeks the malware signature and compares with the stored signature. The anomaly based detection identifies apparent divergences or inconsistencies between the target events and predefined normal transmissions that proposed in [4]. Furthermore, protocol analysis based detection is proposed in which irregular events are distinguished from routine streams in a session by leveraging a pre-determined ubiquitous profile in [5]. These works mainly focus on high layer events or protocols.

The MEC network can also easily obtain the wireless channels, locations and other physical information of users. These information are more difficult to impersonate due to the different propagating in wireless channels. Motivated by this, this paper proposes a physical attributes based spoofing detection mechanism for the MEC network. The channel attributes are unreliable due to the broadcast nature of wireless channel. Therefore, multiple channel attributes are considered and the cluster algorithm are adopted to enhance the detection precision. To further reduce the computational complexity, we also propose an improved cluster algorithm which can achieve nearly optimal performance with extremely low complexity.

II. The Spoofing Detection mechanism

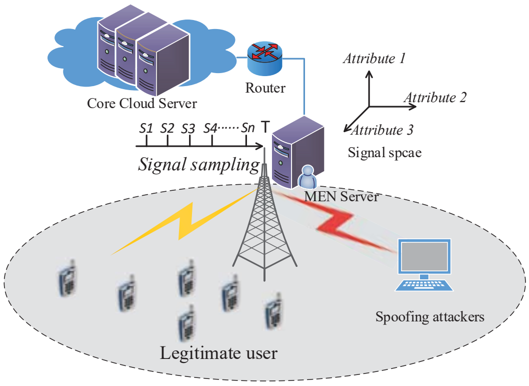

Fig. 1: Architecture of the spoofing detection mechanism.

As is shown in figure 1, the MEC server samples received signals to obtain n sampling objects in a period time T for clustering algorithm. Each sampling object contains multiple channel attributes to build multi-dimension signal space as

$$S_i = [A_1, \cdots A_m] \tag{1}$$

where $A_i (i = 1 \ \cdots m)$ represents one kind of the channel attributes used for intrusion detection. The sampling object

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

number n and the attribute number m jointly determine the detection precision.

In order to simplify the analysis, the received signal strength, direction of arrival signal and channel impulse response are adopted as the detection attributes. These attributes would be clustered through our proposed improved local heuristics algorithm. The cluster results can be obtained to determine the spoofing attacker's number.

The square Euclidean distance between sample object S_i and object S_j can be expressed as

$$d_{ij}^2 = \|S_i - S_j\|_2 \tag{2}$$

The proposed local heuristic algorithm for clustering is as shown in table I. The idea of automatic clustering is based on the System Evolution proposed in [6] in which the all the other clusters are separated if the twin cluster can be separate. The cluster number K_{op} can be obtained from the improved local heuristics based cluster algorithm. The detection mechanism can be summarised as

$$K_{op} \begin{cases} = K_{le} & No\ spoofing\ attack \\ > K_{le} & Exist\ spoofing\ attacks \\ < K_{le} & Missing\ detection \end{cases} \tag{3}$$

The MEC sever would report its security situation to the core cloud server to take countermeasure for spoofing attacks.

TABLE I: The improved local heuristic based cluster algorithm

Step 1	Select the initial medoids M_j using local heuristic algorithm.
Step 2	Assign every sample objects to their nearest medoids
Step 3	Calculate the sum of Euclidean distances from all sample objects to their nearest medoids as follow $J = \sum_{j=1}^{K} \sum_{s_i \in C_j} \|S_i - M_j\|_2$
Step 4	Calculate the cost function as follow $D_j = \sum_{S_i \in C_j} \|S_i - M_j\|_2$
Step 5	Find a new medoid for each cluster set, which is the sample object that minimizing the cost function
Step 6	Assign all sample objects to the new medoids until the J converged to constant.
Step 7	Execute the System Evolution algorithm to get the cluster number.

III. Simulation Results and Analysis

As is shown in figure 2 and figure 3, the improved local heuristics clustering algorithm can achieve near-optimal performance with extremely low computational latency. The simulation platform is MATLAB R2015b with the computer configures Intel(R) Core(TM) i5-3337U cpu 1.8GHz, and 12GB RAM. It is well worthy that compromising little detection performance to achieve extremely low computational complexity in MEC network. The multiple attributes detection can achieve excellent performance compared single attribute detection.

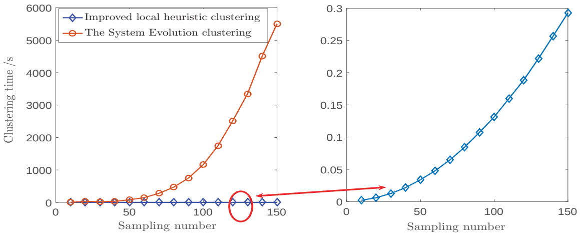

Fig. 2: Clustering Latency.

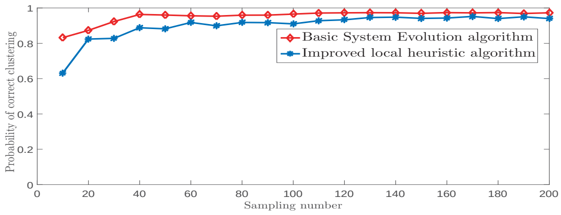

Fig. 3: Clustering Performance.

IV. Conclusion

In this letter, a multiple channel attributes based spoofing detection mechanism is proposed based on the improved local heuristics clustering algorithm. This mechanism is well suitable for MEC network due to the channel attributes could be obtained in real time for MEC service. The multiple channel attributes detection have better performance compared to single attribute detection while the computational complexity also increases extremely high. To reduce the computational complexity, the improved local heuristic based cluster algorithm is proposed to find a near-optimal solution. The simulation results valid the effectiveness of our work.

Acknowledgment

This work is supported by the National Natural Science Foundation for Young Scientists of China (No. 61601051), the Shenzhen science and technology innovation commission free exploring basic research project (No. JCYJ20170307172830043), the Beijing Natural Science Foundation under (No. 4174081).

References

[1] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: Convergence of computing, caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779, 2017.

[2] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016.

[3] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[4] W. Meng, W. Li *et al.*, "Efm: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism," *computers & security*, vol. 43, pp. 189–204, 2014.

[5] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011.

[6] K. Wang, J. Zheng, J. Zhang, and J. Dong, "Estimating the number of clusters via system evolution for cluster analysis of gene expression data," *IEEE Transactions on information technology in biomedicine*, vol. 13, no. 5, pp. 848–853, 2009.