Effective Trust-Based Packet Filtering Method in Collaborative Networks

[1]Sneha K P, [2]Snigdhamol M S

[1] P G Scholar, [2] Assistant Professor,
[1] Department of Electronics and Communication Engineering,
[1] A P J Abdul Kalam Technological University,
[1]Thejus Engineering College, Kerala, India

Abstract : Wireless Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of attacks. Wireless sensor networks (WSNs) are used in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. This paper proposes a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). This method uses two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster'-Shafer theory, which is a mathematical theory of evidence. This method uses an energy efficiency model by using Sleep Wake Scheduling technique in Trust method. This process can achieve more energy consumption and high energy efficiency compared to previous Active Trust model.

IndexTerms - WSN, Attacks, HEIDS, Bayesian inference, Dempster's Shafer Theory, Energy Efficiency

I. INTRODUCTION

In Wireless networks use radio frequencies in air to transmit and receive data instead of using physical cables. The most admiring fact in the networks is that it removes the need for laying out expensive cables and maintenance costs. Setting up a wireless system is easy and fast and it removes the need for pulling out the cables through walls and ceilings. Network can be elongated to places which cannot be wired. Wireless networks offer more flexibility and adapt easily to changes in the configurations of the network. Mobile users especially for Smartphone users are provided with access to real-time information even when they are away from their home or office. WSN is an infrastructure-less self-forming and self-healing network used for voice and data range extension in mission critical applications. A wireless sensor network (WSN) exists of structurally assigned self-governing sensors to monitor environmental or physical conditions, such as sound, pressure, temparature, etc. and to cooperatively pass their data through the network to the destination[1].

Wireless Sensor Networks can vary the topology from a star network to an advanced multi-hop wireless mesh network. The routing or flooding is the propagation technique between the hops of the network. In many surveillance applications of WSN s, tracking a mobile target (e.g., a human being or a vehicle) is one of the main objectives. The discrete detection events a target tracking system is often required to ensure continuous monitoring, i.e., there always exist nodes that can detect the target along its trajectory (e.g., with low detection delay or high coverage level)[2]. Therefore, the most stringent criterion of target tracking is to track with zero detection delay or 100% coverage. Since nodes often run on batteries that are generally difficult to be recharged once deployed, energy efficiency is a critical feature of WSN s for the purpose of extending the network lifetime. If the energy efficiency is enhanced, the quality of service (QoS) of target tracking is highly likely to be negatively influenced. The nodes to sleep may result in missing the passing target and lowering the tracking coverage. Therefore, energy efficient target tracking should improve the tradeoff between energy efficiency and tracking performance e.g., by improving energy efficiency at the expense of a relatively small loss on tracking performance[3].

Wireless sensor networks (WSN s) are widely applied in monitoring, sensing, and collecting the information of interest in the environment. Localization of target nodes is a fundamental problem in wireless sensor networks. Up to now, the most existing localization algorithms of WSNs can be classified into two categories: range-based and range-free. Range-based algorithms use distance or angle estimates in their location estimations. Range-free algorithms use connectivity information between unknown nodes and anchor nodes[4]. Energy use of the sensing device should be decreased and sensor nodes should be energy efficient since their limited energy resource regulates their lifetime. To sustain the power the nodes normally turn off the radio transceiver if it is not in use.

The rest of the paper is organized as follows. Section II presents the related work. Section III explains the proposed model. Section IV presents the simulation results and the paper is concluded in Section V.

II. RELATED WORK

An intrusion detection system (IDS) is a software or device that monitors a network or systems for malicious activity or policy infractions. Any malicious activity or violation is typically reported either to an controller or possessed centrally using a Security Information and Event Management (SIEM) system. Based on different detection methodologies, an IDS can be typically classified as signature-based IDS and anomaly-based IDS. A signature-based IDS [5] or rule-based IDS [6] detects a potential attack by comparing incoming events with its stored signatures, where a signature is a kind of description that defines an attack or an exploit by means of expert knowledge. On the other hand, an anomaly based IDS ([7],[8]) tries to identify great deviations between current events and its pre-established normal profile. A normal profile often represents a normal action or a normal network connection through monitoring the normal behaviour for a long period.

By using string matching, signature-based network intrusion detection systems (NIDSs) [9]can achieve a higher accuracy and lower false alarm rate than the anomaly-based systems. But the matching process is very expensive regarding to the performance of a signature-based NIDS[10] in which the cost is at least linear to the size of the input string and the CPU occupancy rate can reach more than 80 percent in the worst case. This problem greatly limits the high performance of a signature-based NIDS in a large operational network. Packet filter scheme aiming to mitigate this problem. In particular, this scheme incorporates a list technique, namely the blacklist to help filter network packets based on the confidence of the IP domains[11]. Besides, this method will adapt and update the blacklist contents by using the method of statistic-based blacklist generation according to the actual network environment[12].

The architecture consists of two major developed components: the context-aware packet filter that constructs with blacklist packet filter; and the monitor engine that monitors the NIDS and provides the statistical analysis of the network traffic to calculate the confidences of relevant IP addresses. Besides, the monitor engine gives feedback and periodically updates the blacklist packet filter. an adaptive blacklist-based packet filter to reduce packets via a statistic-based method [13], [14]. As the statistic-based method lacks of theoretical basis for generating blacklists, we then developed a trust-based blacklist packet filter using Bayesian inference [15], which was shown to be better than the statistic-based method in the aspects of blacklist false rates and traffic sensitivity.

III. PROPOSED SYSTEM

This paper proposes a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). ActiveTrust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. And an energy efficiency model by using Sleep Wake Scheduling technique in Active Trust method.This paper, using recent advances in uncertain reasoning originated from artificial intelligence community. Mainly two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster'-Shafer theory, which is a mathematical theory of evidence. The energy efficiency model by using Sleep Wake Scheduling technique in Trust method can achieve more energy consumption and high energy efficiency compared to previous Active Trust model.

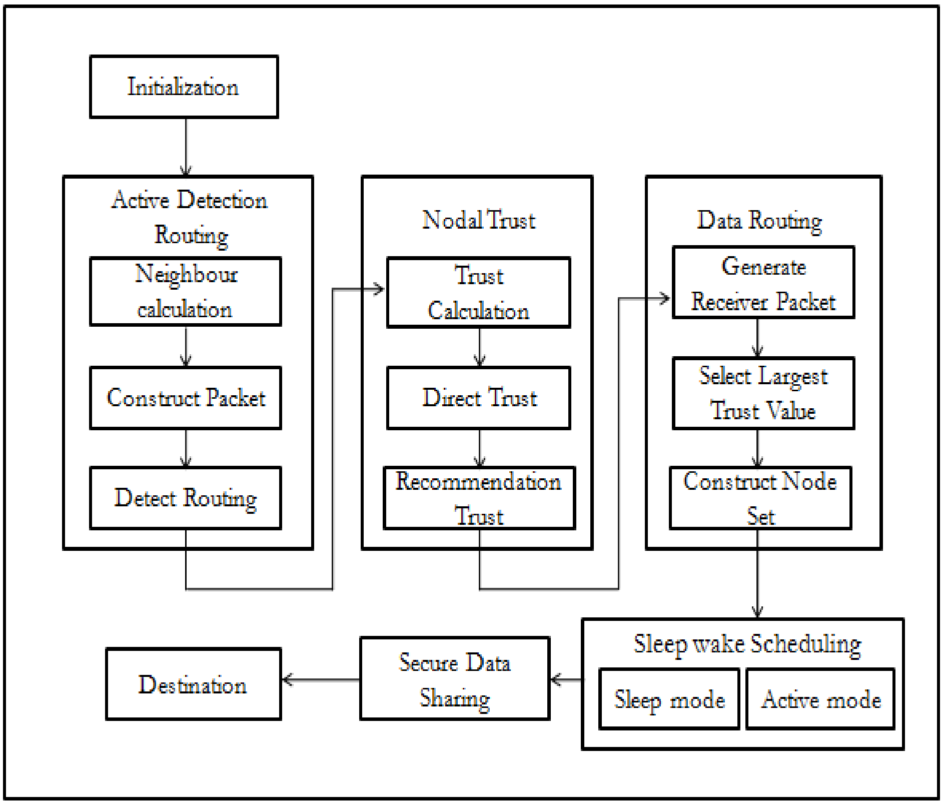

Fig.1.Architecture of proposed system

The system manly consists of four modules:

- Active Detection Routing
- Nodal Trust
- Data Routing
- Sleep Wake Scheduling

The active detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behavior and then mark the black hole location. Hence, the system can lesser the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Over active detection routing, nodal trust can be quickly rapidly, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes. . In this method, the source node inconstantly selects an undetected neighbor node to create an active detection route. Considering that the longest detection route length is w, the detection route decreases its length by 1 for every hop until the length is decreased to 0, and then the detection route ends.

head	type	source	ϖ	ω	id

Fig.2. Detection routing packet

The source node selects an undetected node to launch the detection route. Once the detection packet is received by nodes, the maximum route length is decreased by 1. After that, if is 0, generate a feedback packet and launch a feedback route to the source, and then restore to the initial value. If is not 0, then continue to select the next hop in the same way; otherwise, end the route. The feedback packet is routed back to the data source; because nodes cache the detection route info, the feedback packet is able to return back to the source.

head	type	source	Destination	S-id	id

Fig.3.Feedback packet

Next one is the nodal trust calculation,during data routing and detection routing every node will perform a nodal trust calculation to aid in black hole avoidance. When node A performs a detection route for node B at time it, if the detection data are successfully routed.

$$\begin{cases} C_A^B = \sum_{i=1}^{w}\left\{\left(\Delta_A^B(t_i) \mid \Lambda_A^B(t_i)\right)\cdot \hbar(i)\right\} \big/ w & , \quad w \neq 0 \\ 0 & , \quad w = 0 \end{cases}$$

Nodal direction trust: Consider the trust set of node A to node B during t to be:Nodal recommendation trust: Node A is the trust evaluator, node C is the target of evaluation, and node B is a recommender of A. Consider B A Cto be the direction trust of A to B and C BC to be the direction trust of B to C; then, the recommendation trust of A to C is

$$R_A^C = C_A^B \times C_B^C$$

For the trust of multiple recommendations, the calculation of the recommendation trust from A to B, B to C, etc., until D to E is

$$R_A^E = C_A^B \times C_B^C \times C_C^D \times C_D^E$$

Recommendation trust merging: Consider that the recommender set of node A is AR, in ∈AR and that the recommendation trust of in to node K is , I k A R; then, the merged trust of A to K is

$$U_A^K = \sum_{n_i \in A_n}\left(u_{n_i} R_A^{n_i,k}\right) \; |u_{n_i} = \frac{R_A^{n_i,k}}{\left(R_A^{n_1,k} + R_A^{n_2,k} + \ldots + R_A^{n_{m-1},k} + R_A^{n_m,k}\right)}$$

Comprehensive trust: Comprehensive trust is the total trust, which merges the recommendation trust and direction trust,The comprehensive trust of a node can be computed as follows. After the node launches a detection route, it calculates the direction trust according to Eq. for each received feedback packet.Through interactions,the node obtains the recommendation trust from its neighbors according , and it then calculates the merged trust according to Eq, for the multiple-recommendation trust. Finally, it calculates the comprehensive trust according.

The next section is the data routing it refers to the process of nodal data routing to the sink. The routing protocol is identical to familiar routing protocols in WSNs ; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink.The core idea of data routing is that when any node receives a data packet, it selects one node from the set of candidates nearer the sink whose trust is greater than the preset threshold as the next hop. If the node cannot find any such appropriate next hop node, it will send a feedback failure to the upper node, and the upper node will re-calculate the unselected node set and select the node with the largest trust as the next hop; similarly, if it cannot find any such appropriate next hop, it sends a feedback failure to its upper node. The upper node, working in the same manner, will re-select a different node from among its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink.

The next section is the sleep wake scheduling this module used to initialize the nodes in network topology. And it is used in network topology and topography for network animator window (network window).And it has syntax for create nodes in network animator window. Sensors that are active or asleep are called as surviving sensors and sensors that are malfunctioned or deadlines are called to fail. Sensor modes vary, based upon the active sensors vary at each and every time. So, a method to decide a sleep schedule at each and every key time.

IV. SIMULATION RESULTS

In this work used ns-2 as the network simulator and conducted numerous simulations to evaluate the HEIDS performance. All sensor nodes are randomly scattered with a uniform distribution. The location of the sink is randomly determined. And evaluates the routing performance under scenarios with different numbers of sensor nodes.The current data suggest that such might have been the case for detection accuracy research. Early researchers created experimental designs that appear to have excluded important types of information. Subsequent researchers systematically built upon earlier designs such that an entire literature developed around variations in a single basic design. Although this work has certainly advanced knowledge, this knowledge may be much more limited than it might have been.

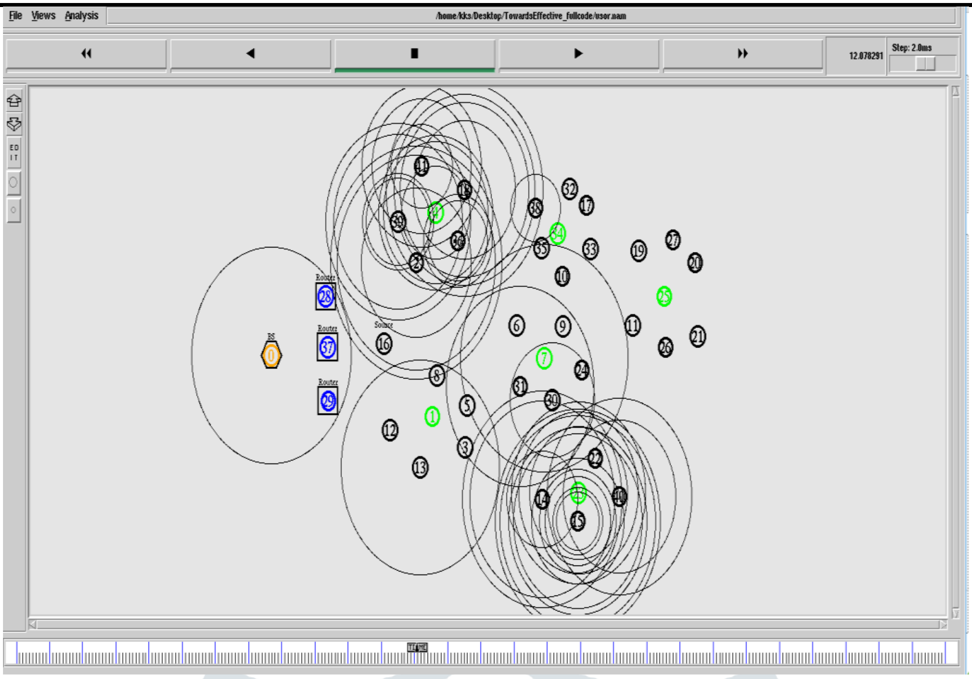

Fig. 4. Graphical representation of simulation window

The theoretical implications of the findings are also multifaceted. Most obviously, the current data are inconsistent with the primacy of the source behavior assumption that is central to much deception theory. Network simulator and conducted numerous simulations to evaluate the WSN performance.

Table .1. Parameter settings

Parameters	Values
Operating System	Ubuntu 10.04
Simulator Tool	NS 2.34
Language	TCL
Protocol Design	C++
MAC protocol	802.11
Number of Mobile nodes	42
Routing protocol	AODV
Time of simulation end	52ms
Data Rate	11Mb

This work evaluates the following main performance metrics:

1) Packet Delivery ratio: measures the mean rate of the packet sending and receiving then calculate delivery ratio.

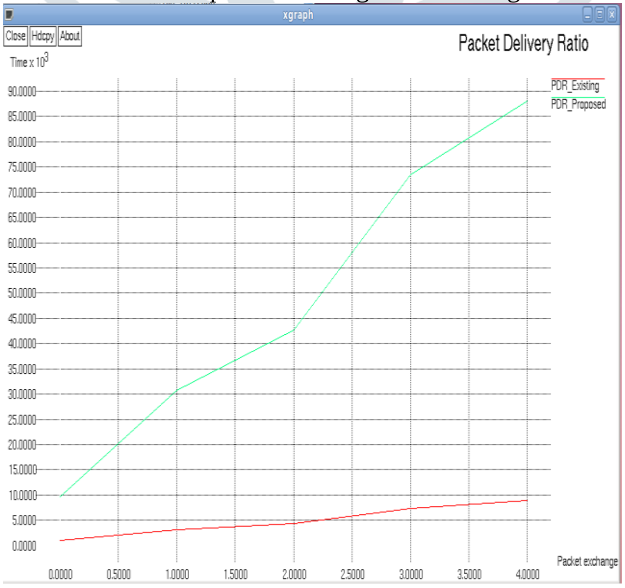

Fig. 5. Comparison of packet delvary ratio

2) Data transmission speed: Means the data packets transferring speed between the nodes.

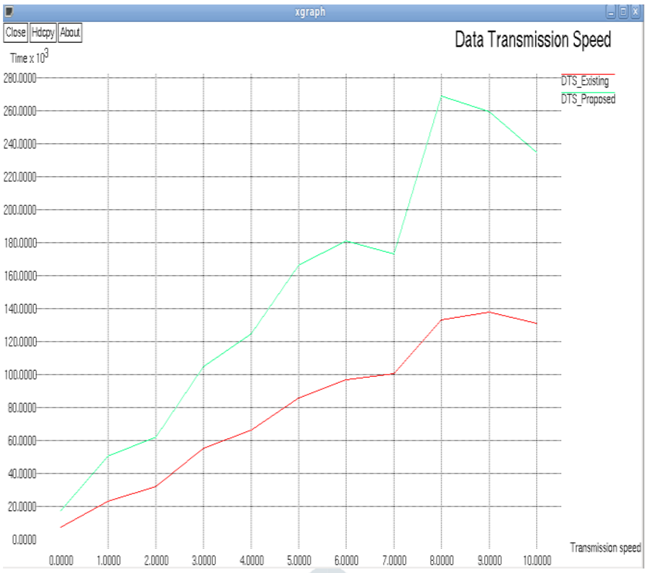

Fig. 6. Comparison of Data transmission speed

3) End-to-end Delay: means the time delay experienced by the source node while transmitting a report message to the sink.

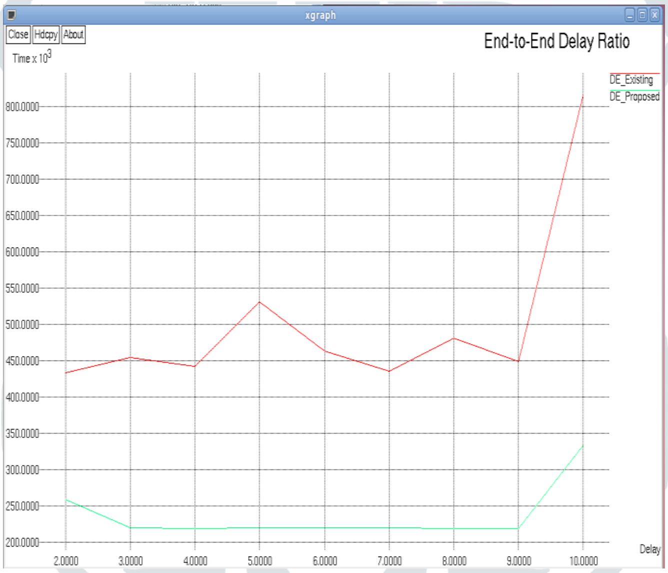

Fig. 7. Comparison of End to End delay ratio

4) Throughput ratio: Measures data sharing and successive ratio rate.

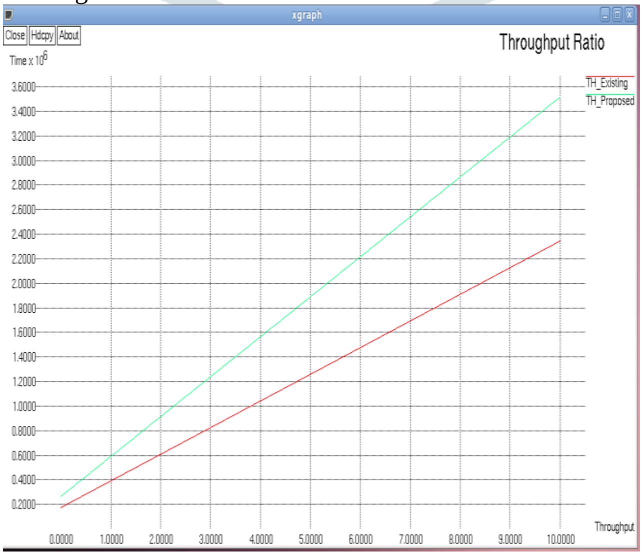

Fig. 8. Comparison of Throughput Ratio

V. CONCLUSION

Here proposed a trust management scheme that enhances the security in networks name Hybrid and Efficient Intrusion Detection Systems (HEIDS). Here used two frameworks for Trust Calculation and Decision Making process. The trust value is derived using Bayesian Inference, and Decision Making based on Dempster'-Shafer theory, which is a mathematical theory of evidence. And an energy efficiency model by using Sleep Wake Scheduling technique in Trust method. And can achieve more energy consumption and high energy efficiency compared to previous Active Trust model. The proposed a security and trust routing scheme based on active detection, and it has the following excellent properties: High successful routing probability, security and scalability. The Trust scheme can rapidly notice the nodal trust and then escape suspicious nodes to rapidly achieve a nearly 100% successful routing probability.High energy efficiency. The Trust scheme fully uses residue energy to construct multiple detection routes. The theoretical search and experimental outcome have shown that the scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, the scheme improves both the energy efficiency and the network security performance.

REFERENCES

[1] N. Roseveare and B. Natarajan, "A structured approach to optimization of energy harvesting wireless sensor networks", IEEE Consumer Communications and Networking Conference (CCNC), pp. 420-425, Las Vegas, 2013.

[2] E. Belding-Royer, "Hierarchical routing in ad hoc mobile networks", Wireless Communications and Mobile Computing, Vol.2, No.5, pp. 515-532, 2002.(REPT

[3] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Hawaii International Conference on System Sciences, Vol. 8, Citeseer, pp. 802, 2000.(REPT 7)

[4] O. Younis, M. Krunz and S. Ramasubramanian, "Node clustering in wireless sensor networks: recent developments and deployment challenges", IEEE Network, Vol. 20, No.3, pp. 20-25, 2006.(REPT 2)

[5] P.A. Porras and R.A. Kemmerer, "Penetration state transition analysis:A rule-based intrusion detection approach," In:Proceedings of the 8th Annual Computer Security Applications Conference (ACSAC), pp. 220- 229, 1992.

[6] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," In: Proceedings of the 13th Large Installation System Administration Conference (LISA), pp. 229-238, 1999.

[7] A.K. Ghosh, J. Wanken, and F. Charron, "Detecting Anomalous and Unknown Intrusions Against Programs," In: Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC), pp. 259- 267, 1998.

[8] A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES," Technical Report, SRI International, January 1995.

[9] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks 31(23-24), pp. 2435-2463, 1999.

[10] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Pevention Systems (IDPS)," NIS Special Publication 800- 94, Feb 2007.

[11] A.V. Aho and M.J. Corasick, "Fast pattern matching: an aid to bibliographic search," Communications of the ACM 18, pp. 333-340, 1975.

[12] R.L. Rivest, "On the worst-case behavior of string-searching algorithms," SIAM Journal on Computing, pp. 669-674, December 1977.

[13] Y. Meng and L.-F. Kwok, "Adaptive Context-aware Packet Filter Scheme using Statistic-based Blacklist Generation in Network Intrusion Detection," In: Proceedings of the 7th International Conference on Information Assurance and Security (IAS), pp. 74-79, 2011.

[14] Y. Meng and L.-F. Kwok, "Adaptive Blacklist-based Packet Filter with A Statistic-based Approach in Network Intrusion Detection," Journal of Network and Computer Applications, vol. 39, pp. 83-92, 2014.

[15] Y. Meng, L.-F. Kwok, and W. Li, "Towards Designing Packet Filter with A Trust-based Approach using Bayesian Inference in Network Intrusion Detection," In: Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SECURECOMM), pp. 203-221, 2012.