Enhancing Blackslist-based Packet Filtration using Blockchain in Wireless Sensor Networks

Wenjuan Li[1,2], Weizhi Meng[1,3], Yu Wang[1⋆], and Jin Li[1]

[1] Institute of Artificial Intelligence and Blockchain, Guangzhou University, China
[2] Department of Computing, The Polytechnic University of Hong Kong, China
[3] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark

Abstract. A wireless sensor network (WSN) consists of distributed sensors for monitoring network status and recording data, which is playing a major role in Internet of Things (IoT). This type of wireless network is driven by the availability of inexpensive and low-powered components. However, WSN is vulnerable to many kinds of attacks like Distributed Denial of Service (DDoS) due to its dispersed structure and unreliable transmission. In the literature, constructing a suitable distributed packet filter is a promising solution to help mitigate unwanted traffic. While how to ensure the integrity of exchanged data is a challenge as malicious internal node can share manipulated data to degrade the effectiveness of filtration. In this work, we design a blockchain-based blacklist packet filter with collaborative intrusion detection that can be deployed in WSNs. The blockchain technology is used to help build a robust blacklist for reducing unwanted traffic. In the evaluation, we investigate the performance of our filter with a real dataset and in a practical WSN environment. The results demonstrate that our proposed filter can enhance the robustness of blacklist generation.

Keywords: Wireless Sensor Network, Distributed Denial-of-Service Attack, Blockchain Technology, Network Security, Packet Filtration.

1 Introduction

A wireless sensor network (WSN) is usually composed of distributed autonomous devices with sensors to monitor environmental conditions in a collaborated manner. It can be considered as the backbone of Internet of Things (IoT) environment, by transmitting data and offering access points for connection [31]. Each WSN node is typically equipped with a radio transceiver or some kind of wireless communication device, e.g., a small microcontroller [20]. WSN has been applied in many fields such as intelligent transportation [22], smart city [37], agriculture [39] and so on. The global industrial WSN market size was expected to reach 94.21 billion USD by the end of 2025 [1].

⋆ Corresponding author, yuwang@gzhu.edu.cn

The relatively simple functioning makes WSNs easy to implement, but due to the unreliable transmission and the distributed structure, WSN is vulnerable to many attacks such as Sybil attack [25], spoofing attack, betrayal attack [34], and Distributed Denial of Service (DDoS) attacks [19]. For example, DDoS attacks can quickly consume the energy of WSN nodes and disrupt the normal functions provided by these sensor nodes [5, 10].

To mitigate these potential risks, intrusion detection system (IDS) is a basic and important security mechanism [17]. Basically, an IDS can be categorized as rule-based detection and anomaly-based detection. The former needs to make a signature matching between the current events and the signature database. The latter needs to build a normal profile and then to compare it with current profile. To fit the distributed network structure, distributed and collaborative intrusion detection has been deployed, which can enhance the detection performance by allowing different detection nodes exchanging required data and information [24, 34]. However, due to the resource constraint, many existing security solutions are unsuitable for WSNs. Thus, more lightweight intrusion detection is demanded for protecting WSNs.

Motivation and Contributions. In the literature, constructing an appropriate packet filter (deployed with a detector) is a promising solution for WSNs to reduce unwanted traffic. For instance, Meng et al. [33] introduced a trusted packet filter in a distributed environments, which can build a blacklist via trust management. However, cyber attackers may have a chance to share misleading information by compromising one or more internal nodes. It is a big challenge on how to secure the integrity of shared data.

For this issue, blockchain technology is a potential solution that can help build a shared and immutable ledger. In this work, we aim to design a blockchain-based blacklist packet filter based on some prior work [29, 32], which can reduce unwanted traffic under attacks. Our contributions can be summarized as follows.

- We introduce a blockchain-based blacklist packet filter, which consists of a blacklist packet filter, a monitor engine and a collaboration component. It can be integrated with collaborative intrusion detection and help refine traffic for WSN nodes. The blacklist generation is based on a weighted ratio-based statistical method.
- The use of blockchain aims to help establish a communication among different nodes without a trusted third party, as well as protect the integrity of shared data that would be used for building a robust blackslist.
- We evaluate the performance of our designed packet filter with a real dataset and in a real WSN under DDoS attack (external attack) and betrayal attack (insider attack). The experimental results demonstrate the effectiveness and robustness of our filter to reduce unwanted traffic in hostile conditions.

The remaining parts are structured as follows. We introduce the design of blockchain-based blacklist packet filter including its major components in Section 2. Section 3 investigates the performance of our packet filter under attacks and analyzes the experimental results. Section 4 introduces related research s-

tudies on intrusion detection in WSNs and packet filter construction. Section 5 concludes our work.

2 Our Approach

This section briefly introduces the background on blockchain technology and details our proposed blockchain-based blacklist packet filter.

2.1 Blockchain Background

With the popularity of bitcoin, blockchain technology has received much attention from both academia and industry. Such technology can be used for monitoring public health data, tracking donation, securing supply chains and more. The blockchain market surpassed 488 million USD in 2018 and was expected to climb to over 39 billion USD by 2025 [2].

Generally, blockchain can be considered as an open, distributed ledger that can record transactions among parties in a verifiable and efficient way. The blockchain structure contains a list of blocks with two major data items: a pointer that records the location information of next block, and data organized in an order. The first block, called Genesis block, is the first record in the blockchain. Each block includes a number of different transactions, previous block hash, timestamp and transaction root [35]. Due the benefits provided by blockchain, it has been applied in may fields, such as healthcare industry [7], intrusion detection [36], intelligent transportation [16] and more.

There are three main types of blockchain: a) *public blockchain* indicates that the data and access to the system is available to anyone like Ethereum [3], b) *private blockchain* indicates that the data and access is given by users from a specific organization or authorized users like Hyperledger [4], and c) *consortium blockchain* indicates the data and access is given by preliminary assigned users. To add a block to the chain, a consensus algorithm is often pre-agreed among all participants. If each node verifies the block and checks whether the information is correct, then the block is added to the chain.

2.2 Blockchain-based Blacklist Packet Filter

Packet filtration is a promising solution to protect WSN nodes, while how to ensure the shared data is still a challenge on constructing an effective distributed packet filter. In this work, we focus on a type of blacklist packet filter from prior work [29, 32, 33] due to its lightweight computation. Motivated by the benefits of blockchain technology, we develop a blockchain-based blacklist packet filter that can be robust to data tempering. Figure 1 depicts the high-level structure of our proposed packet filter, including three major components: collaboration component, trust management component and blacklist packet filter.

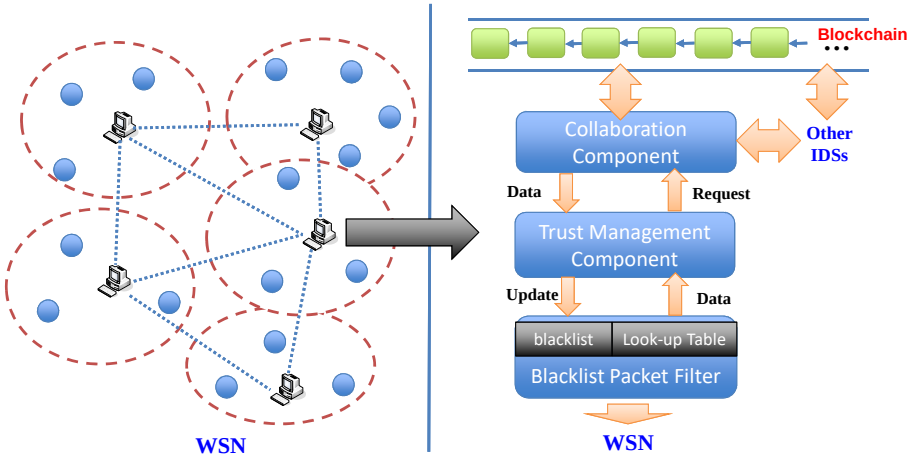

Fig. 1. The high-level review of blockchain structure.

- *Collaboration component.* This component is responsible for connecting with other IDS nodes and gathering the required information for computing the IP reputation and generating the blacklist. For the local IDS, the trust management component can send a request to this component and exchange the information with target nodes.
- *Trust management component.* This component is a key component with the purpose of generating the blacklist based on the collected information. It has to calculate the IP reputation and update the list regularly. In a CIDS environment, this component can request the data from target nodes.
- *Blacklist packet filter.* This component is mainly used to reduce traffic based on the IP reputation. It includes two parts: a blacklist and a look-up table. The former contains all blacklisted IP addresses (for unwanted packet reduction), and the latter indexes all IDS signatures by the blacklisted IP addresses (for process acceleration).

Filter workflow. The incoming traffic should first reach the *blacklist packet filter*. If the IP address of the packet matches one in the blacklist, then the filter will further compare the payload of this packet with the signatures in its *look-up table* (contains all active IDS signatures).

- If a match is identified, then the blacklist packet filter can block this packet and generate an alert. Meanwhile, a short message will be sent to the monitor engine, reporting the IP address as malicious.
- On the other hand, if the payload of the packet does not match any signatures, then this packet will be sent to the internal network directly.

WSN with collaborative intrusion detection. In such WSN, CIDSs are used to protect the security of sensor nodes. Similar to a cluster head, each CIDS manages the blacklist packet filter for several WSNs (as shown in Figure 1). Each

CIDS can exchange information with other nodes in order to collect required information for computing IP reputation and generating the blacklist.

Weighted Ratio-based blacklist generation. The blacklist-based packet filter uses a weighted ratio-based method to compute the IP reputation as shown in Equ. (1), where i represents the total number of *good* packets, k represents the total number of *bad* packets and W is the weight value.

$$IP\ reputation = \frac{i}{\sum_1^k W \times k} \quad (i, k \in \mathbf{N}) \tag{1}$$

Blockchain layer. To ensure the integrity of shared data, a consortium blockchain is used to identify malicious data provided by CIDS nodes. CIDS nodes would only accept the data / information that has been verified by chain nodes. Thus, the blockchain can be only expanded if the majority of nodes have agreed that the received data is trustful.

3 Evaluation

In this section, we conduct two experiments to investigate the performance of our proposed blacklist-based packet filter. The consortium blockchain was deployed in a mid-end computer with Intel(R) Core (TM)i6, CPU 2.5GHz with 500 GB storage. There is a need for 2/3 nodes in the network to sign a block to be appended to the blockchain.

- *Experiment-1.* We use a real dataset captured from a honeynet environment (with five-day data) to explore the reduced time consumption between our filter and the original one.
- *Experiment-2.* We collaborated with an IT organization and investigate the filter performance under adversarial WSN scenarios with DDoS attack and betrayal attack.

To facilitate the comparison with previous work [29, 32], we set the threshold as 1, the weight value as 10, and the update time was 5 seconds (which allows the blacklist packet filter to complete all required operations regarding blacklist generation and updating).

3.1 Experiment-1

We constructed a real dataset captured from a Honeynet project (`https://www.honeynet.org/tag/hong-kong/`) with the *base rate* [6] of around 0.003937. It consists of five-day incoming network traffic (denote as *DAY1*, *DAY2*, *DAY3*, *DAY4* and *DAY5*), with around 4-6 million packets each day [32]. The packets in the dataset were labeled as either *normal* or *attack* by means of expert knowledge.

Table 1. The reduced time consumption between the original blacklist packet filter and our proposed filter.

Week Day (Original Filter - normal)	*DAY1*	*DAY2*	*DAY3*	*DAY4*	*DAY5*
Reduction rate (%)	24.61	28.65	**30.42**	22.56	32.32
Week Day (Original Filter - attack)	*DAY1*	*DAY2*	*DAY3*	*DAY4*	*DAY5*
Reduction rate (%)	24.61	28.65	**26.56**	**17.83**	**26.37**
Week Day (Our Filter - attack)	*DAY1*	*DAY2*	*DAY3*	*DAY4*	*DAY5*
Reduction rate (%)	24.61	28.65	**30.42**	22.56	32.32

To explore the performance between the original filter and our proposed filter, we manipulated some false data in *DAY3*, *DAY4* and *DAY5* to influence the blacklist generation. Table 1 shows the reduced time consumption between the original filter and our proposed filter under normal and attack conditions. It is found that our proposed packet filter would not affect the performance of the original one (*DAY1* and *DAY2*), but can enhance its security under attack condition (from *DAY3* to *DAY5*). For example, due to the attack, the original filter had an obvious decrease of filtration rate from *DAY3* to *DAY5*, compared to the normal performance. By contrast, our proposed filter can be robust to such type of attack thanks to the usage of blockchain (i.e., malicious data would be rejected if major nodes does not accept it).

3.2 Experiment-2

To investigate the practical performance of our proposed filter, we worked with an IT organization (in Southern China) and conducted an experiment in a WSN environment with 35 CIDS nodes. We particularly launched two attacks: DDoS (flooding attack) and betrayal attack (where a trusted internal node becomes malicious), and observed the impact on both the network and our filter. The former aims to decrease the bandwidth while the latter aims to degrade the effectiveness of blacklist by sending false data.

The experiment was repeat three times and we adopted two metrics: average false positive rate (AFR) and average false negative rate (AFN), which are average values of false positives and false negatives.

Table 2. The average false positive rate (AFR) and average false negative rate (AFN) regarding the generation of blacklist.

Metric	*Original Filter*	*Our Filter*
AFP (%)	16.4	6.32
AFN (%)	18.6	7.83

Table 2 shows that under adversarial conditions, the original filter would suffer a high false rate of generating blacklist (with AFP 16.4% and AFN 18.6%).

Especially, the insider attack can cause a high false negative rate, so that the filter is ineffective in reducing unwanted traffic. In comparison, our proposed filter could reach an AFP of 6.32% and an AFN of 7.83%, demonstrating that our filter can enhance the security of blacklist generation. This is because the blockchain technology can help secure the integrity and authenticity of shared data. The malicious input would be rejected due to the consensus process among all CIDS nodes.

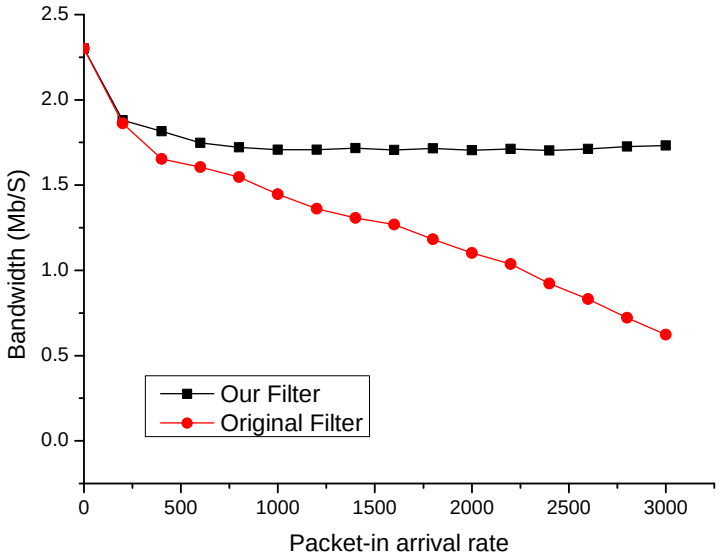

Fig. 2. The impact of flooding DDoS attacks on the network bandwidth between our filter and the original filter.

Figure 2 depicts the impact of flood DDoS attacks on the network bandwidth between the original filter and our filter, using the tool (`https://www.netscantools.com/nstpro_packet_generator.html`). It is observed that the bandwidth had a clear decrease under the original filter, i.e., the bandwidth decreased to below 1 when the packet-in arrival rate reached 2400 packets/s. In contrast, our filter could be robust against malicious input and protect the blacklist generation via the blockchain technology. Under our filter, the bandwidth could be maintained at around 1.7. The experimental results overall demonstrate the viability and effectiveness of our proposed filter.

3.3 Discussion

The use of blockchain in constructing a packet filter is not new in the literature. For instance, Kolokotronis et al. [21] proposed a collaborative trust-based packet filter, in which the trust calculation engine continuously updates the blacklist

by collecting alerts from the detector and side information from the CIDS peers. However, they did not show any experimental results on the filter performance. In this work, we detail the design of our blockchain-based packet filter and analyze its performance with a real dataset and in a real WSN environment. Below are some open challenges that can be addressed in our future work.

- *Blockchain platform.* In our current work, we only use a demo blockchain system to realize our filter and explore its performance. In future work, we plan to consider a real blockchain platform such as Ethereum and Hyperledger and validate the performance.
- *Security threats and attacks.* In this work, we explore the filter performance under DDoS attack and betrayal attack. The results demonstrate the effectiveness of blockchain-based approach, while some other attacks could be considered in future, including advanced insider attacks such as fingerprinting attack [26].
- *Communication workload.* The blockchain can bring many benefits in protecting the data integrity, but it may also cause more delay and overhead during the consensus process (depending on the consensus algorithms). This is an important topic in our future studies.
- *Trust management in blacklist generation.* How to build trust is very important to generate a robust blacklist that can be used in the packet filter. In this work, we adopt a weighted ratio-based blacklist generation method, which can provide a false rate around 7-9% in the real WSN environment. In future, we plan to consider other trust management models (e.g., Bayesian model [31]) and investigate the filtration performance.

4 Related Work

This section introduces related research work regarding intrusion detection in WSNs and the construction of software or hardware-based packet filter.

4.1 Intrusion Detection in WSNs

To protect WSNs from security threats, intrusion detection has been widely studied. Chen et al. [12] focused on the security of WSNs and introduced a protocol to construct a trust framework model called ETSN. The trust value relies on different events of a sensor node in WSNs, and would be distributed based on the radio range of the sensor. Wang et al. [41] introduced IDMTM - Intrusion Detection Mechanism based on the Trust Model, which could help detect malicious nodes by collecting evidence from locally and the neighboring nodes. Dang et al. [13] introduced a Trusted Intrusion Detection System (TIDS) with double cluster heads and many cluster members for WSNs. There are a kind of monitoring nodes that are responsible for collecting the information and evaluating the credibility of cluster nodes. Han et al. [15] aimed to design a low-consumption IDS to detect malicious attacks for WSNs, based on game

theory and an autoregressive model. It could consider energy consumption during detection process and select a balanced strategy between detection efficiency and cost. Bai et al. [9] presented a detection algorithm based on the changing rates of multiple attributes (CRMA), which can detect multiple attacks. The CRMA values could be calculated by minimizing the weighted deviation via convex optimization. If the deviation of Observed Change Rate exceeds the threshold, then an alarm can be made.

Trust management is an important solution to build a trust-based collaborative intrusion detection system (CIDS) for WSNs and distributed networks. For instance, Li et al. [24, 25] designed a intrusion sensitivity-based CIDS and assigned the value via machine learning classifiers. The use of intrusion sensitivity can enhance the detection accuracy of malicious nodes. Ma et al. [27, 28] proposed a Distributed Consensus based Trust Model (DCONST), which could detect multiple-mix-attacks and evaluate the trustworthiness of nodes by sharing certain information called cognition. More related work on WSN-related IDSs can refer to a survey [11].

4.2 Packet Filtration

Due to the computing resource and energy constrains, many existing security mechanisms are not suitable for WSNs. Thus, constructing a packet filter is a lightweight security solution to reduce malicious or unwanted traffic. Meng and Kwok [29, 32] introduced a context-aware blacklist packet filter, which generated the blacklist using a weighted ratio-based approach. The results demonstrated that the filter could be effective to reduce the IDS burden in processing network packets without affecting the whole security level. Then they introduced a list packet filter using both whitelist and blacklist technique. Meng et al. [33] proposed a collaborative trust-based packet filter that could achieve robust trust computation and effectively reduce unwanted traffic. They defined a metric of overall IP confidence to represent the overall trustworthiness of an IP source. Trabelsi et al. [40] designed a hybrid mechanism based on both splay tree filters and pattern-matching algorithms to enhance IDS packet filtering, allowing early packet rejection or acceptance.

In addition to software-based packet filtration, many research focuses on hardware-assisted packet filtration. Sourdis et al. [38] selected only a small portion from each IDS rule to be matched in the pre-filtering step and then built a hardware-based pre-filtering solution with multiple processing engines. Leogrande et al. [23] pointed out that existing filtering expressions is too complex and introduced pFSA, which used finite state automata to ensure the optimal number of checks on the packets without sacrificing filtration time. Fiessler et al. [18] identified that complex rules requiring software-based processing may be interleaved at arbitrary positions and introduced HyPaFilter+, a hybrid classification system with an FPGA-based hardware matcher to reach a simple but effective hardware and software packet filtration. Durante et al. [14] introduced a formal model for networks including multiple cascaded firewalls, which can enable the transfer of a set of rules from a firewall to its downstream neighbors

when the changes in the input traffic profile. The transformation algorithm can preserve the security integrity of the network while moving rules between cascaded firewalls, allowing tangible performance improvements in terms of packet processing rate for a given traffic profile.

While for distributed packet filtration, how to ensure the authenticity and integrity of shared data is a challenge, which motivates our work in designing a blockchain-based blacklist packet filter.

5 Conclusion

WSN is an important part of IoT environments, which can be used to monitor the environmental status and changes. While WSN is vulnerable to various attacks like DDoS attacks. To mitigate the unwanted traffic, this work proposes a blockchain-based blacklist packet filter. The use of blockchain technology is motivated by its capability of ensuring data integrity, and the use of blacklist is due to its wide adoption in practice. In the evaluation, we investigate the performance of our filter with a real dataset and in a practical WSN environment under DDoS attack and betrayal attack. It is found that, as compared with the original filter, our proposed filter can be more robust against malicious input and protect the blacklist generation process.

Acknowledgments. This work was partially supported by National Natural Science Foundation of China (No. 61802080 and 61802077).

References

1. Wireless Sensor Network Market - Forecast (2021 - 2026) (Access on Feb 2021) https://www.industryarc.com/Report/211/Wireless-Sensor-Network-Market-Research-Report.html
2. Size of the blockchain technology market worldwide from 2018 to 2025. (Access on March 2021) https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/
3. Ethereum - open-source blockchain. https://ethereum.org/en/
4. Hyperledger C Open Source Blockchain Technologies. https://www.hyperledger.org/
5. A.P. Abidoye, I.C. Obagbuwa: DDoS attacks in WSNs: detection and countermeasures. IET Wirel. Sens. Syst. 8(2), pp. 52-59 (2018)
6. S. Axelsson, The Base-Rate Fallacy and the Difficulty of Intrusion Detection, ACM Transactions on Information and System Security 3(3), pp. 186-205 (2020)
7. E.J. De Aguiar, B.S. Fai?al, B. Krishnamachari, J. Ueyama: A Survey of Blockchain-Based Strategies for Healthcare. ACM Comput. Surv. 53(2), pp. 27:1-27:27 (2020)
8. F. Bannour, S. Souihi, A. Mellouk: Adaptive distributed SDN controllers: Application to Content-Centric Delivery Networks. Future Gener. Comput. Syst. 113, pp. 78-93 (2020)

9. H. Bai, X. Zhang, F. Liu: Intrusion Detection Algorithm Based on Change Rates of Multiple Attributes for WSN. Wirel. Commun. Mob. Comput. 2020, pp. 8898847:1-8898847:16 (2020)
10. M.H. Bhuyan, N.A. Azad, W. Meng, C.D. Jensen. Analyzing the Communication Security between Smartphones and IoT based on CORAS. In: Proceedings of the 12th International Conference on Network and System Security (NSS), pp. 251-265, 2018.
11. I. Butun, S.D. Morgera, R. Sankar: A Survey of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Commun. Surv. Tutorials 16(1), pp. 266-282 (2014)
12. Chen, H., Wu, H., Hu, J., Gao, C.: Event-based Trust Framework Model in Wireless Sensor Networks. In: Proceedings of the 2008 International Conference on Networking, Architecture, and Storage (NAS), pp. 359-364 (2008)
13. N. Dang, X. Liu, J. Yu, X. Zhang: TIDS: Trust Intrusion Detection System Based on Double Cluster Heads for WSNs. In: Proceedings of WASA, pp. 67-83 (2019)
14. L. Durante, L. Seno, A. Valenzano: A Formal Model and Technique to Redistribute the Packet Filtering Load in Multiple Firewall Networks. IEEE Trans. Inf. Forensics Secur. 16, pp. 2637-2651 (2021)
15. L. Han, M. Zhou, W. Jia, Z. Dalil, X. Xu: Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Inf. Sci. 476, pp. 491-504 (2019)
16. M. Humayun, N.Z. Jhanjhi, B. Hamid, G. Ahmed: Emerging Smart Logistics and Transportation Using IoT and Blockchain. IEEE Internet Things Mag. 3(2), pp. 58-62 (2020)
17. K. Hutchison: Wireless Intrusion Detection Systems. SANS GSEC Whitepaper, 1-18 (2005) `http://www.sans.org/readingroom/whitepapers/wireless/wireless-intrusion-detection-systems1543`
18. A. Fiessler, C. Lorenz, S. Hager, B. Scheuermann, A.W. Moore: HyPaFilter+: Enhanced Hybrid Packet Filtering Using Hardware Assisted Classification and Header Space Analysis. IEEE/ACM Trans. Netw. 25(6), pp. 3655-3669 (2017)
19. O. Kasim: An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. Comput. Networks 180: 107390 (2020)
20. I. Khan, F. Belqasmi, R.H. Glitho, N. Crespi, M. Morrow, P. Polakos: Wireless Sensor Network Virtualization: A Survey. IEEE Commun. Surv. Tutorials 18(1), pp. 553-576 (2016)
21. N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis, S. Shiaeles: On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection. In: Proceedings of SERVICES, pp. 21-28 (2019)
22. F. Kong, Y. Zhou, G. Chen: Multimedia data fusion method based on wireless sensor network in intelligent transportation system. Multim. Tools Appl. 79(47), pp. 35195-35207 (2020)
23. M. Leogrande, F. Risso, L. Ciminiera: Modeling Complex Packet Filters With Finite State Automata. IEEE/ACM Trans. Netw. 23(1), pp. 42-55 (2015)
24. W. Li, W. Meng, L.F. Kwok. Design of Intrusion Sensitivity-Based Trust Management Model for Collaborative Intrusion Detection Networks. In: Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM), pp. 61-76 (2014)
25. W. Li, W. Meng. Enhancing Collaborative Intrusion Detection Networks Using Intrusion Sensitivity in Detecting Pollution Attacks. Information and Computer Security, vol. 24, no. 3, pp. 265-276 (2016)

26. W. Li, W. Meng, L.F. Kwok, H.H.S. Ip. Developing Advanced Fingerprint Attacks on Challenge-based Collaborative Intrusion Detection Networks. Cluster Computing, vol. 21, no. 1, pp. 299-310 (2018)
27. Z. Ma, L. Liu, W. Meng. DCONST: Detection of Multiple-Mix-Attack Malicious Nodes Using Consensus-based Trust in IoT Networks. In: Proceedings of the 25th Australasian Conference on Information Security and Privacy (ACISP), p-p. 247C267, 2020.
28. Z. Ma, L. Liu, W. Meng. Towards Multiple-Mix-Attack Detection via Consensus-based Trust Management in IoT Networks. Computers & Security, vol. 96, 101898 (2020)
29. Y. Meng, L.F. Kwok: Adaptive context-aware packet filter scheme using statistic-based blacklist generation in network intrusion detection. In: Proceedings of the IAS, pp. 74-79 (2011)
30. Y. Meng, L.F. Kwok: Enhancing List-based Packet Filter Using IP Verification Mechanism against IP Spoofing Attack in Network Intrusion Detection. The 6th International Conference on Network and System Security (NSS), pp. 1-14 (2012)
31. Y. Meng, W. Li, L.F. Kwok. Evaluation of Detecting Malicious Nodes Using Bayesian Model in Wireless Intrusion Detection. In: Proceedings of the 7th International Conference on Network and System Security (NSS), pp. 40-53 (2013)
32. Y. Meng, 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)
33. W. Meng, W. Li, L.F. Kwok. Towards Effective Trust-based Packet Filtering in Collaborative Network Environments. IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 233-245 (2017)
34. W. Meng, F. Fei, W. Li, M.H. Au. Evaluating Challenge-based Trust Mechanism in Medical Smartphone Networks: An Empirical Study. In: Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM), pp. 1-6 (2017)
35. W. Meng, J. Wang, X. Wang, J.K. Liu, Z. Yu, J. Li, Y. Zhao, S.S.M. Chow. Position Paper on Blockchain Technology: Smart Contract and Applications. The 12th International Conference on Network and System Security (NSS), pp. 474-483 (2018)
36. W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han. When Intrusion Detection Meets Blockchain Technology: A Review. IEEE Access, vol. 6, no. 1, pp. 10179-10188 (2018)
37. J.P.J. Peixoto, D.G. Costa: Wireless visual sensor networks for smart city applications: A relevance-based approach for multiple sinks mobility. Future Gener. Comput. Syst. 76, pp. 51-62 (2017)
38. I. Sourdis, V. Dimopoulos, D.N. Pnevmatikatos, S. Vassiliadis: Packet pre-filtering for network intrusion detection. In: Proceedings of ANCS, pp. 183-192 (2006)
39. D. Thakur, Y. Kumar, A. Kumar, P.K. Singh: Applicability of Wireless Sensor Networks in Precision Agriculture: A Review. Wirel. Pers. Commun. 107(1), pp. 471-512 (2019)
40. Z. Trabelsi, S. Zeidan, M.M. Masud: Network Packet Filtering and Deep Packet Inspection Hybrid Mechanism for IDS Early Packet Matching. In: Proceedings of AINA, pp. 808-815 (2016)
41. Wang, F., Huang, C., Zhang, J., Rong, C.: IDMTM: A Novel Intrusion Detection Mechanism based on Trust Model for Ad-Hoc Networks. In: Proceedings of the 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 978C984 (2008)