Unifying Trust-Aware Network Attacks from a Machine Learning Security Perspective

Tanmayee Deshprabhu (University of Oxford), Justin P Coon (University of Oxford)

1 Abstract

It has been predicted that future communications will be highly dependent on distributed networks in both private and public settings. There are some outstanding challenges regarding the security of distributed networks, particularly in Internet-of-Things (IoT) systems, due to the lack of a central management entity to oversee all the interactions. Trust and reputation will play a significant role in providing distributed security to these networks by allowing each node to evaluate the reliability and/or intention of each other node in the network based on observational data. However, the current literature on trust networks has a disjointed view of the possible threats and uses varying terminology to describe the basic malicious attack models. In this article, we attempt to unify the attack models into a core framework based on a survey of recent literature, with a focus on early-stage prevention of trust network attacks.

2 Introduction

In the last decade, there has been rapid growth in mobile data traffic as a result of the increasing number of connected devices and the desire for fast, automated and easily accessible mobile communications. As a result of these requirements, there has been significant scientific research in using distributed network systems such as Internet of Things (IoT) networks [1]. The decentralization of communication networks means that the network functionality and size are no longer limited by the capabilities of some central entity. Additionally, IoT distributed networks allow more ad-hoc communication networks, thereby enabling a vast range of applications that were previously not possible with the traditional communications framework. However, there are still a number of challenges with providing security and accountability to communications in distributed networks.

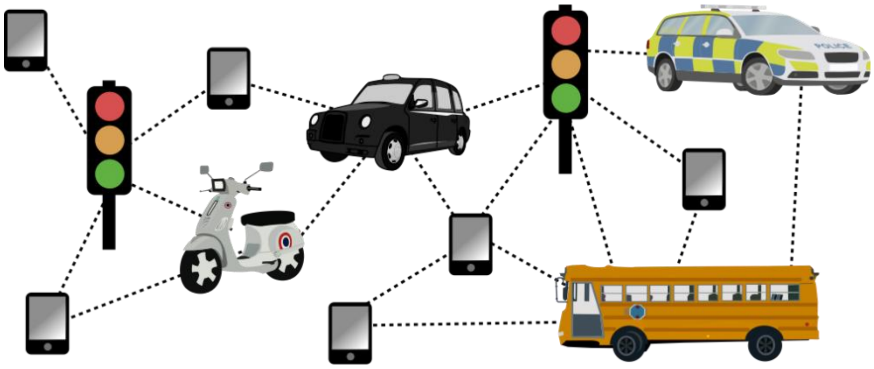

Figure 1. Example of an IoT network for traffic communications.

The absence of a central authority in a distributed system means that the nodes need to be able to independently assess the reliability of data and of other nodes. *Trust inference* aims to achieve this and provides a useful tool for each node to independently carry out its own risk assessment based on past observations. There is also interest around integrating artificial intelligence (AI), specifically machine learning techniques, alongside trust in order to account for more complex malicious attacks on communication networks. Supervised machine learning algorithms, such as support vector machines (SVM), can be used to categorize new data based on past and similar scenarios [2]. Being able to characterize and profile node behavioral patterns using these techniques would allow for malicious activity to be flagged based on the behavior leading up to a network attack. This forms part of our future work, where we will aim to create a framework for early and efficient detection of network attacks in distributed communication systems.

In the following sections, we identify the problem of classifying trust-based network attacks and present a survey of the recent literature on these attacks, which unifies terminology and concepts into a simple classification table. We then provide a possible characterization framework for malicious nodes based on these network attacks and, lastly, a discussion on machine learning techniques to proactively detect and prevent the attacks.

2.1 The Problem

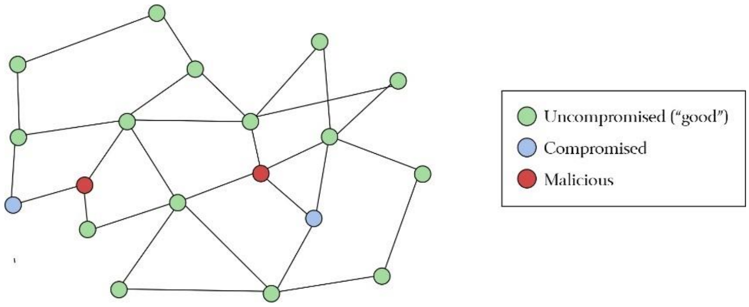

Figure 2. An example of a distributed communication network with two attacking nodes.

Some past reviews of trust inference from a more general perspective are available, [3] [4] [5]. However, as a result of varying terminology across the literature and hundreds of minor variations on the core attack models, there is an unclear view of the threats that any particular trust-based security protocol should seek to detect. Secondly, many trust inference models tend to address a specific attack. Targeting a small set of threats is likely to result in a higher accuracy for tier 1 nodes, but tier 2 and tier 3 malicious nodes would be able to detect and work around the targeted security. Finally, many of the attacks discussed in the literature rely heavily on the malicious node already having achieved significant trust. This is especially true with the Denial-of-Service (DoS) class of attacks.

Our ultimate goal is to identify the trends in behavior of nodes executing particular attacks, which would allow us to take on a preventative approach at an early stage, rather than waiting for a large-scale attack such as DoS to happen. Attacks like DoS, flooding, Sybil, etc. can be prevented by addressing the early-stage tactics of an attacker.

It is important to note that the nodes in an IoT system are typically resource-constrained and an intrusion detection system would need to account for this in its complexity. [6] provides an example of low-power detection of more general network attacks but does not take into consideration any form of early detection, whilst [7] uses an early detection approach for low-power devices but does not consider the full range of trust attacks. Being limited by device capability and power, the detection process needs to find a balance between the range of attacks that can be detected and the resources that are spent in trying to look for the specific attacks. However, having a clear view of the attack categories greatly helps to reduce the overhead on a network by effectively narrowing the search space of the attack detection process.

We can see from these issues that there is a need for a clearer view of the key threats that an AI-assisted system should be able to identify. Therefore, our contributions are:

(i) We present a survey of recent literature (since 2017) on trust inference and reputation-based attacks and, using this, we identify the key attack modes of a trust-aware malicious node.
(ii) We provide a discussion on characterization of malicious nodes that conduct these attacks based on the survey of literature, with a view to using machine learning-based profiling and classification to proactively prevent these attacks in trust networks.

3 Overview of Trust

Trust is defined as the probability that the next time one observes a particular node, that node will behave as one expects it to. The trustworthiness, or simply trust, that a node A has about node B is based on a set of previous observations A holds about B. An observation can comprise of any interaction that A has had with B in the network, such as data exchanges, speed of response, monetary transactions, etc. Observations can also be second-hand, but relayed observations need to be adjusted based on the trust of the relaying nodes.

There is extensive work on trust inference and different ways to calculate trust from an observation set. Some approaches take a statistical Bayesian approach by calculating the probability density function of the trust based on a set of positive and negative observations, with a widely-used example being the Beta Reputation System [8]. Another option is to consider the data being received from the observee and to calculate the trust based on the entropy of the data [9].

Table 1. Categories of malicious nodes in a trust environment.

Category	Description
Tier 1: Naïve malicious nodes	Attacker commits malicious actions without consideration of how these actions will affect its trust rating nor for how its trust rating will limit the disruption caused by its actions.
Tier 2: Passive trust-aware malicious nodes	Attacker follows a protocol which maximizes the effect of its malicious actions on the network, e.g., by behaving well initially to build up a good reputation.
Tier 3: Adaptive trust-aware malicious nodes	Same as Tier 2 but the malicious node is able to learn about the network's trust inference framework and periodically changes its attack mode to evade detection.

Table 1 shows the different types of malicious nodes that can be present in a network, where the tiers 1-3 are categorized by how aware the malicious node is about the type of trust inference that the network is using to protect itself. The majority of trust inference models can swiftly detect naïve malicious nodes, or tier 1 in Table 1, which are nodes that carry out their attack without consideration or knowledge of the trust inference security in place. For example, a naïve malicious node may enter a network and immediately start spreading false information. Its trust rating would quickly decrease and its actions would then have a negligible effect on the network operation. The naïve malicious node is not realistic, however, as a determined attacker would likely be aware of the trust inference security in place.

The concept of trust is also embedded in our everyday IT systems. On e-commerce platforms such as online marketplaces and on-demand taxi apps, people typically use the *user rating* of an account to decide whether they should complete a transaction with that account. Having recognized this, malicious parties have been known to invoke ways of increasing their own rating. Similarly, in network trust, nodes with higher ratings tend to have a greater effect on the network functionality and group decisions. In a wireless sensor network using data collation, the input from trusted nodes would typically be amplified to have a greater effect on the final result while the input from untrustworthy nodes would be attenuated. Thus, many of the trust-aware attack protocols within tier 2-3 in Table 1 rely on maximizing the malicious node's reputation relative to the honest nodes in the network prior to committing a malicious action.

4 Survey of trust inference attack modes (2017 to present)

We conducted a review of trust inference literature since 2017 and collated the trust-aware attacks that have been discussed in each work. As we are looking at these from a prevention and machine learning standpoint, it is important to categorize the attacks and identify the key threats that would be of interest to a preventative security algorithm.

In Table 2, we can see that there is a wide range of terminology used to refer to the threats. We have collated this into clear categories of attack, combining minor variations and alternate names from across the reviewed works.

4.1 Early-Stage Attacks

There are four early-stage attack modes: false identity, collusion, on-off and false trust reporting. These are the attack modes that exist only within the trust inference environment because their protocols specifically manipulate the trust ratings of the network in order to maximise the effect of the attack on the network. These attacks often precede one or more of the leveraged attacks. They are of key interest from a machine learning security perspective because, by detecting these, one can seek to prevent the disruptive part of the attack, such as the 'off' stage in an on-off attack.

4.2 Leveraged Attacks

Leveraged attacks are those that do not directly involve the manipulation of reputations. For example, the false data reporting in Table 2 can form part of the other attacks such as the 'off' stage in the on-off attack but, generally, the various false data reporting attacks can happen independently of trust inference and are classed as tier 1 in Table 1.

The resource-limiting category in Table 2 consists of attacks on the network or node resources specifically, whilst the false data reporting category contains attacks that affect the data directly.

Taking possession of another node can also be classed as a leveraged attack because this can be carried out independently of a trust inference network as the main goal in this protocol is to evade detection. Let us say that the goal becomes to preserve the malicious node's trust rating whilst carrying out the attack through a compromised node. Then from a machine learning detection perspective, this would appear much like collusion in terms of the node interactions and characteristics. Lastly, there are attacks where a node attempts to limit the resources of the network. These can also occur in most types of communication networks and rely on the malicious node already having established a position within the network whereby it can have an effect on the network functions. It is often too late by this point to take on a preventative security approach.

Table 2. Survey of attack models in trust inference literature (2017-present)

Attack type	Attack name	Protocol	Minor variations and alternative names	Citation
Early-stage attack: involving manipulation of reputations				
False identity	**White-washing**	Having committed a malicious action resulting in low trust, the node leaves and re-joins the network with a new identity to reset its reputation.	Newcomer, node replication	[10], [11], [12], [13], [14], [15] , [16], [17], [18], [19], [20], [21], [22], [23]
	Sybil	A node joins the network under a false identity to evade detection.	False identity	[24], [25], [14], [20], [21], [22], [23], [26], [27]
Collusion		Two or more nodes work in collaboration to achieve a high trust for at least one of the nodes.	Ballot-stuffing, orchestrated, time-varying attack, wormhole attack	[28], [29], [13], [30], [15], [20], [22], [23], [31], [32], [33], [34], [35], [36]
On-off		The node behaves normally in the network for a period of time to achieve a high trust ('on' phase) and then executes a malicious action ('off' phase), thereby maximizing the effect of that action on the network.	Conflicting behavior, garnishing, sleeper, camouflage	[10], [28], [37], [29], [11], [24], [19], [20], [34], [38], [39] [40], [41], [42], [43], [44], [45], [46],
False trust reporting	**Slandering**	The node C consistently relays bad observations about another node in the network D, resulting in D having a significantly lower trust.	Bad-mouthing, time-varying attack, ballot-stuffing, false validation, defamation	[28], [37], [29], [24], [30], [15], [18], [23], [31], [32], [34], [36], [26], [45], [46], [47], [27]
	Self-promotion	The node relays positive observations about itself to other nodes in the network to improve its own reputation.	Selfish attack	[24], [30], [15], [18], [23], [31], [40], [26]
Leveraged attack: not specific to trust networks				
Resource-limiting	**Denial of service**	The node creates a high demand on the network resources such that they become unavailable to other nodes and the network function is disrupted.		[24], [48], [43]
	SSDF Attack	The node sends false information to the channel regulator / base station about whether the channel is in use.		[49], [50], [51]
False data reporting	**Black hole**	The node drops all (black hole) or some (grey hole) packets that it receives	Sinkhole, concealment, selective forwarding	[19], [52], [14], [53], [54], [55], [32], [56], [44], [45], [46], [27]
	Tampering	The node changes existing data without permission.		[57], [24], [58], [14], [18], [32], [33], [34], [35], [27]

	Forgery	The node creates new, falsified data.		[24], [14], [18]
	Replay	The node repeats an out-of-date or invalidated packet		[19], [14]
Taking possession of another node	**Man-in-the-middle**	The node compromises another node and uses its resources or reputation to carry out a malicious action	Eavesdropping	[24], [59], [60], [51]
	Discrimination	Any attack in which the malicious node takes advantage of another node's bad reputation or low trust rating		[18], [20]

5 Characterization

5.1 Attack characteristics

Machine learning classification algorithms rely heavily on pattern recognition for decision making. Based on the survey of trust-aware attacks in the literature above, we have identified the characteristics of nodes that would be most likely to commit these attacks.

Many software providers gain access to information about a device by running a smaller program on the device prior to executing. This is prevalent in multiplayer online video games, where the information-seeking program is called an anti-cheat and is used to monitor any secondary activity on the device that occurs while the main software is running, with the aim of identifying potential malicious activity i.e., cheating. Similar technology has been picked up by video conferencing programs and has recently started to be adapted for use in IoT [61].

Considering false identity attacks, in which the attacker frequently leaves and re-joins the network in order to refresh its trust rating, we can say confidently that its network connection length is likely to be shorter than average. Secondly, its trust rating would never reach a stable high given that new nodes tend to be assigned a neutral rating such as 0.5 in most trust models. Therefore, just before an attack, the node is likely to have a neutral-to-low trust rating and will have been in the network for a short period of time.

Table 3. Characterising nodes that would be most likely to commit each trust-aware network attack.

ATTACK	**NODE CHARACTERISTICS**			
	Node capability Can be measured in a number of ways	**Trust** Reputation, trust probability, etc.	**Network Connection Length** How long the node has been participating in the network	**Reach** How many others the node has communicated with
False Identity	-	Low	Short	-
ON-OFF	-	High	-	Frequent communication with a large number of nodes
Collusion	Low	-	-	Frequent communication with a small number of nodes
False Trust Reporting	-	High	Long	Frequent communication with a large number of nodes
Example network scenario: ad-hoc, distributed IoT network at a public café. Typical nodes would include mobile phones, laptops, street infrastructure nodes such as smart traffic lights, etc.				
Example metric, range	Processing power, 0.2 – 150 MIPS.	Trust probability, 0-1.	Time spent within network range, 0 – 180 minutes.	Frequency of transactions*, 0-60 per minute. Number of nodes contacted 0-20 nodes.
Example definition of threshold	Small: <50 MIPS Large: >120 MIPS	Low: <0.6 High: >0.9	Short: <10 minutes Long: >1 hour	Frequent: >20 per minute Large number of nodes: >10

* If the frequency threshold is met then depends on the number of nodes being contacted regularly.

Similarly, for the on-off attack, the malicious node seeks to achieve a high trust rating as soon as possible to leverage the 'off' phase of its attack. Therefore, it would attempt to communicate with many nodes and with high frequency to raise its trust rating in the eyes of the other nodes. Just before switching to the 'off' phase, it would have achieved a notable increase in its trust rating as the result of interacting with many nodes in a short period of time. A slanderer is likely to follow similar behavioral patterns, but is more likely to seek an even higher trust rating. This is because the slanderer seeks to have an effect on ratings that are two or more hops away in the network, which requires a higher rating than the simpler on-off attack. Therefore, it is likely that the network connection length of a slanderer would also tend to be longer.

If a less powerful node, such as a lightweight IoT device, wishes to maximise its effect on the network, then it is most likely to participate in a collusion-based attack. This would involve frequently communicating with its colluders.

These attacker characteristics are summarized in Table 3, with an example given at the end for a public local area network. The specific thresholds would need to be adapted for a particular application and can then be used to form training data for supervised machine learning algorithms.

5.2 Implementation of ML Techniques using characterization

By collating, categorizing and understanding the key threats to a trust inference network, the aim is to create a unified framework of threats for future work on trust-based security models. We hope that this will provide a foundation upon which to build realistic training data for attack prevention algorithms using supervised machine learning techniques, as demonstrated by Figure 3.

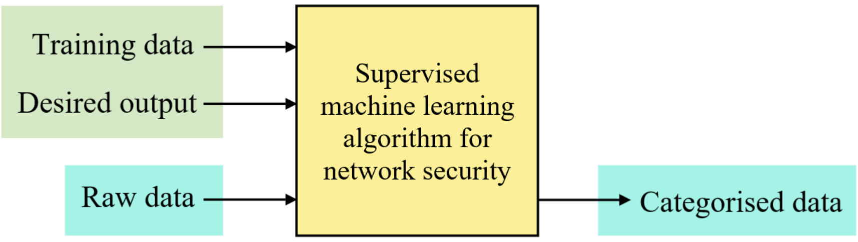

Figure 3. The nature of supervised machine learning algorithms.

Supervised machine learning algorithms can utilize labelled training data to identify trends and patterns in new, previously unseen data. This is one of the key directions of machine learning security research. In a trust network scenario, the observations that each node holds about other nodes can already be considered as labelled data. Past bad observations can form the training data for detecting future issues with a particular node. Being able to attach more information to the bad observations and attacks, such as the node characteristics, would allow the algorithm to identify other nodes that are likely to commit the same attack in the future.

6 Conclusion

In this article, we have presented a survey of recent literature on attacks in trust and reputation networks. The survey was categorized, from a machine learning classification perspective, into a clear summary of the network threats that should be addressed by a trust-based security system. We have also discussed the application of machine learning to detect possible network attacks in their early stages by profiling node behaviors. Our future work will focus on developing the attack-specific node characteristics into training data for machine learning classification algorithms, and subsequently to observe how successfully the attacks can be detected and prevented.

7 Acknowledgment

The authors wish to acknowledge the support of the Bristol Research & Innovation Laboratory of Toshiba Europe Ltd.

8 Bibliography

[1] S. Naveen and M. R. Kounte, "Key Technologies and challenges in IoT Edge Computing," in *Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019.

[2] K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan and J. A. Chambers, "Support Vector Machine for Network Intrusion and Cyber-Attack Detection," in *Sensor Signal Processing for Defence Conference (SSPD)*, 2017.

[3] D. D. S. Braga, M. Niemann, B. Hellingrath and F. B. D. L. Neto, "Survey on Computational Trust and Reputation Models," *ACM Computing Surveys,* vol. 51, pp. 1-40, 2018.

[4] Y. Ruan and A. Durresi, "A survey of trust management systems for online social communities – Trust modeling, trust inference and attacks,," in *Knowledge-Based Systems*, 2016.

[5] J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models," in *Artificial Intelligence Review*, 2005.

[6] G. S. Dhunna and I. Al-Anbagi, "A Low Power Cyber-Attack Detection and Isolation Mechanism for Wireless Sensor Network," in *IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017.

[7] M. M. I. M. I. I. Z. M. H. M. Hasan, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things,* vol. 7, 2019.

[8] A. Josang and R. Ismail, "The Beta Reputation System," in *5th Bled Electronic Commerce Conference*, 2002.

[9] Y. Gong and L. Chen, "Trust Evaluation of User Behavior Based on Entropy Weight Method," in *International Conference on Computer Engineering and Networks*, 2020.

[10] J. Zhang, K. Zheng, D. Zhang and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," *in IEEE Access,* vol. 8, pp. 21077-21090, 2020.

[11] I. T. Javed, K. Toumi, F. Alharbi, T. Margaria and N. Crespi, "Detecting Nuisance Calls over Internet Telephony Using Caller Reputation," *Electronics,* vol. 10, p. 353, February 2021.

[12] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussain, "MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles," *IEEE Internet of Things Journal,* vol. 7, pp. 3310-3322, April 2020.

[13] L. Liu, Z. Ma and W. Meng, "Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks," *Future Generation Computer Systems,* vol. 101, pp. 865-879, December 2019.

[14] G. Arulkumaran and R. K. Gnanamurthy, "Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network," *Mobile Network Applications,* vol. 24, pp. 386-393, 2019.

[15] A. Gruner, A. Muhle, T. Gayvoronskaya and C. Meinel, "A Quantifiable Trust Model for Blockchain-based Identity Management," in *IEEE International Conference on Internet of Things (iThings)*, 2018.

[16] K. A. Awan, I. U. Din, A. Almogren and H. Almajed, "AgriTrust—A Trust Management Approach for Smart Agriculture in Cloud-based Internet of Agriculture Things," *Sensors,* vol. 20, p. 6174, October 2020.

[17] K. Rabadiya, A. Makwana and S. Jardosh, "Revolution in networks of smart objects: Social Internet of Things," in *Conference: 2017 International Conference on Soft Computing and its Engineering Applications*, 2017.

[18] O. A. Wahab, R. Cohen, J. Bentahar, H. Otrok, A. Mourad and G. Rjoub, "An endorsement-based trust bootstrapping approach for newcomer cloud services," *Information Sciences,* vol. 527, pp. 159-175, 2020.

[19] S. Ji, H. Ma, Y. Liang, H. Leung and C. Zhang, "A whitelist and blacklist-based co-evolutionary strategy for defensing against multifarious trust attacks," *Applied Intelligence,* vol. 47, pp. 1115-1131, 2017.

[20] M. Faisal, S. Abbas and H. U. Rahman, Identity attack detection system for 802.11- based ad hoc networks, EURASIP Journal on Wireless Communications and Networking, 2018.

[21] X. Meng, "speedTrust: a super peer-guaranteed trust model in hybrid P2P networks," *The Journal of Supercomputing,* vol. 74, pp. 2553-2580, June 2018.

[22] M. Wang, C. Qian, X. Li and S. Shi, "Collaborative Validation of Public-Key Certificates for IoT by Distributed Caching," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019.

[23] A. Ugur, "Manipulator: A Novel Collusion Attack on Trust Management Systems in Social IoT," *Proceedings of 10th Computer Science On-line Conference,* vol. 1, pp. 578-592, 2021.

[24] W. Fang, W. Zhang, Y. Yang, Y. Liu and W. Chen, A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution, in Science China: Information Sciences, 2017.

[25] R. Casadeia, A. Aldinib and M. Virolia, "Towards attack-resistant Aggregate Computing using trust mechanisms," *Science of Computer Programming,* vol. 167, August 2018.

[26] D. Velusamy and G. K. Pugalendhi, "Fuzzy integrated Bayesian Dempster-Shafer theory to defend cross-layer heterogeneity attacks," *Information Sciences,* vol. 479, pp. 542-566, 2019.

[27] A. Amouri, V. T. Alaparthy and S. D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things," *Sensors,* vol. 20, January 2020.

[28] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng and X. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology,* vol. 68, pp. 7108-7120, July 2019.

[29] K. A. Awan, I. U. Din, A. Almogren, H. Almajed, I. Mohiuddin and M. Guizani, NeuroTrust -Artificial Neural Network-based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things, IEEE Internet of Things Journal, 2020.

[30] D. Mehetre, E. Roslin and S. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," *Cluster Computing,* vol. 22, January 2019.

[31] V. B. Reddy, S. Venkataraman and A. Negi, "Communication and Data Trust for Wireless Sensor Networks Using D-S Theory," *IEEE Sensors Journal,* vol. 17, pp. 3921-3929, June 2017.

[32] W. Yong-hao, "A Trust Management Model for Internet of Vehicles," in *Proceedings of the 2020 4th International Conference on Cryptography*, 2020.

[33] W. Fang, N. Cui, W. Chen, W. Zhang and Y. Chen, "A Trust-Based Security System for Data Collection in Smart City," *IEEE Transactions on Industrial Informatics,* vol. 17, pp. 4131-4140, June 2021.

[34] J. You, J. Shangguan, L. Zhuang and N. Li, "An Autonomous Dynamic Trust Management System with Uncertainty Analysis," *Knowledge-Based Systems,* vol. 161, 2018.

[35] S. Nie, "A novel trust model of dynamic optimization based on entropy method in wireless sensor networks," *Cluster Computing,* vol. 22, pp. 11153-11162, 2019.

[36] V. Suryani, V. Sulistyo and W. Widyawan, "Two-phase security protection for the Internet of Things," *Journal of Information Processing Systems,* vol. 14, pp. 1431-1437, December 2018.

[37] S.-s. Zhang, S.-w. Wang, H. Xia and X.-g. Cheng, "An Attack-Resistant Reputation Management System For Mobile Ad Hoc Networks," *Procedia Computer Science,* vol. 147, pp. 473-479, 2019.

[38] W. Li, W. Meng and L. Kwok, "SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks," vol. 10232, 2017.

[39] J. Caminha, A. Perkusich and M. Perkusich, "A smart middleware to detect on-off trust attacks in the Internet of Things," in *IEEE International Conference on Consumer Electronics (ICCE)*, 2018.

[40] J. Caminha, A. Perkusich and M. Perkusich, A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things, Security and Communication Networks, 2018.

[41] J. Fan, Q. Li and G. Cao, "Privacy Disclosure through Smart Meters: Reactive Power Based Attack and Defense," in *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017.

[42] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang and J. J. P. C. Rodrigues, "FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things," *IEEE Access,* vol. 7, pp. 13476-13485, 2019.

[43] A. M. Kowshalya and M. L. Valarmathi, "Trust Management in the Social Internet of Things," *Wireless Personal Communications: An International Journal,* vol. 96, pp. 2681-2691, September 2017.

[44] F. Khedima, N. Labraouia and A. A. A. Ari, "A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks," *Journal of Network and Computer Applications,* vol. 123, pp. 42-56, December 2018.

[45] C. V. Mendoza and J. H. Kleinschmidt, "A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach," *Wireless Personal Communications: An International Journal,* vol. 103, pp. 2501-2513, December 2018.

[46] M. D. Alshehri, F. K. Hussain and O. K. Hussain, "Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT)," *Mobile Network Applications,* vol. 23, pp. 419-431, June 2018.

[47] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh and M. Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Computers and Electrical Engineering,* vol. 72, pp. 894-909, November 2018.

[48] R. E. Navas, H. L. Boulder, N. Cuppens, F. Cuppens and G. Z. Papadopoulos, "Demo: Do Not Trust Your Neighbors! A Small IoT Platform Illustrating a Man-in-the-Middle Attack," 2018.

[49] Y. Fu and Z. He, "Bayesian-Inference-Based Sliding Window Trust Model Against Probabilistic SSDF Attack in Cognitive Radio Networks," *IEEE Systems Journal,* vol. 14, pp. 1764-1775, June 2020.

[50] W. Fang, C. Zhu, W. Chen, W. Zhang and J. J. P. C. Rodrigues, "BDTMS: Binomial Distribution-based Trust Management Scheme for Healthcare-oriented Wireless Sensor Network," vol. 2018, pp. 382-387, 2018.

[51] F. Zhao, S. Li and J. Feng, Securing Cooperative Spectrum Sensing against DC-SSDF Attack Using Trust Fluctuation Clustering Analysis in Cognitive Radio Networks, in Wireless Communications and Mobile Computing, 2019.

[52] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali and S. Begum, VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead, Cost-Effective Techniques for Sensors Technology, 2018.

[53] S. G. Fatima, S. K. Fatima and S. I. A. Sattar, "A Security Scheme based on Trust Attack in MANET," *International Journal of Advanced Research in Engineering and Technology,* vol. 10, April 2019.

[54] N. J. Patel and K. Tripathi, "Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method," *International journal of scientific research in science, engineering and technology,* vol. 4, pp. 281-287, 2018.

[55] S. Xie, Z. Zheng, W. Chen, J. Wu, H. Dai and M. Imran, "Blockchain for cloud exchange: A survey," *Computers and Electrical Engineering,* vol. 81, 2020.

[56] X. Liu, Y. Liu, A. Liu and L. T. Yang, "Defending ON–OFF Attacks Using Light Probing Messages in Smart Sensors for Industrial Communication Systems," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 9, pp. 3801-3811, 2018.

[57] H. Alhumud, M. Zohdy, D. Debnath and R. Olawoyin, Cooperative Spectrum Sensing for Cognitive Radio-Wireless Sensors Network Based on OR Rule Decision to Enhance Energy Consumption in Greenhouses, Wireless Sensor Network, 2019.

[58] J. Jia and Y. Li, "A trust attack detection algorithm based on improved K-means clustering," *IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC),* pp. 1996-2004, 2020.

[59] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni and Y. Yang, Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey, in Wireless Communications and Mobile Computing, 2020.

[60] M. H. Junejo, A. Rahman, R. Shaikh, K. M. Yusof, I. Memon, H. Fazal and D. Kumar, A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks, Sci. Program, 2020.

[61] A. Dolan, I. Ray and S. Majumdar, "Proactively Extracting IoT Device Capabilities: An Application to Smart Homes," 2020.