Journal of Engg. Research Vol. 9 No. (2) June 2021 pp. 92-105 https://doi.org/10.36909/jer.v9i2.8837

Innovative survey of defense machinery against Sybil attacks over wireless ad hoc network on IoT

Arun Kumar Singh

Asst. Professor, College of Computing and Informatics, Saudi Electronic University, Kingdom of Saudi Arabia, KSA
a.singh@seu.edu.sa, arunsinghiiita@gmail.com

Submitted: 17/10/2019
Revised: 10/10/2020
Accepted: 19/10/2020

ABSTRACT

Integrating IoT with Wireless Ad hoc Network (WANET) capabilities can solve several problems. However, because they both rely on identity nodes to communicate with each other, they are both vulnerable to Sybil attacks. Sybil attackers illegally change into several different identities (attackers) to carry out various malicious activities such as damaging data aggregation, voting, and disrupting routing. Several defense machineries have been proposed for Sybil attacks on WANET, which are mostly based on cryptography, location or position, network behavior, resource testing, and trust. However, the drawbacks are that not all machinery are suitable for use in networks with limited resources. This paper presents a survey, classification, and comparison of various defense machineries that have been proposed for non-IoT WANETs. The author emphasizes the issue of the advantages and disadvantages of this defense mechanism when applied to the IoT infrastructure and how each method can effectively recognize properties of Sybil attacks.

Keywords: Sybil Attack; Wireless Ad Hoc Network; Internet of things.

INTRODUCTION

Internet of Things (IoT) is a technology where devices get a particular identity to be able to connect and communicate with one another through internet networks without human-to-human or human-to-machine interactions. A collection of IoT devices connected by a network is called IoT infrastructure. It is grouped into four layers, i.e., sensors and actuators, internet gateway and data acquisition system, edge handler, and data center. Sensors and actuators are used to collect data from the environment or physically observed objects. Units of sensors and actuator are what we call nodes. Nodes can communicate with each other using specific protocols to produce this useful set of data. Analog data from sensors and actuators are converted into a digital form by data acquisition devices, which is then forwarded by the internet gateway to Edge handler layer. Edge handler function is to prevent data from the edge to consume data center bandwidth. It also can process raw data into data that is ready to be processed. The last layer is Data Center and Cloud; at this layer, data is processed and analyzed in depth for later use by its users.

In contrast to the current paradigm on the Internet, which is based on human-to-human relations, Gutiérrez (Reina DG et al., 2013) mentioned that IoT has a paradigm as the future internet, and every physical or virtual object that can be identified with unique identifiers will be considered to be interconnected (Lu Ta et al., 2010). So, keeping this in mind, although IoT uses distributed networks in nature, IoT has driven combinations with other technologies, such as short-range communication, real-time localization, embedded sensors, and ad hoc networks as a way to turn everyday things into smart things.

Combining IoT with an ad hoc network provides benefits because of the ad hoc properties as self-organized networks. They are built spontaneously by several connected devices. The nodes together build a unicast or multicast communication as a flow of messages, rather than relying on a router or base station, so they are suitable for implementation where the deployment of new fixed infrastructure is not feasible.

In addition, when the mobility characteristic is calculated, making it a Wireless Ad hoc Network, the Wireless Ad hoc Network itself represents a new communication paradigm where decentralized wireless nodes communicate with each other in collaborative ways to achieve common goals. So, considering the many capabilities owned by Wireless Ad hoc Network, it would be highly beneficial to IoT, and this will also be suitable for implementations that require mobility.

On the other hand, there is something to be considered in the integration of these two technologies. As both depend on the node that communicates using particular identities, both are still facing common security problems. It is vulnerable to Sybil attacks. A Sybil attack is defined as an intrusion where malicious devices get or change into several different identities illegally. Based on its characteristics, Sybil attack is grouped into the identity-based attack, in which both attacks compromised the system using false identities. This type of attack disguises themselves as legitimate devices, and it is done by attacker camouflaging its intrusion packet data similar to regular data packets. The security system would find it difficult to distinguish between the two types of data packages. For detecting this kind of attack, a lot of traditional countermeasures is proposed. However, adopting traditional security countermeasure cannot effectively be used in IoT due to its source limitation. Along with the many studies regarding the method of securing Sybil attacks on the Wireless Ad Hoc Network, the question that arises is related to what are the methods used in the IoT defense mechanism and what is the drawbacks? Similar questions have been investigated by Vasudeva A. et al. (2018) and Newsome J. et al. (2004) with both focusing on non-IoT infrastructure. In this paper, researches related to machine learning on IoT security are collected from various sources and then reviewed using the Systematic Literature Review method (Kitchenham B et al., 2009). The main focus would be the compatibility of the current Sybil defense mechanism in Wireless Ad hoc Networks, considering its integration in IoT infrastructure that has limitation in the resource. So, the aim of this paper is to present a survey of security mechanism that has been proposed for Wireless Ad Hoc Network to get the results of the analysis, methods of which are suitable, and what needs to be taken into account in the implementation of security machinery in IoT is that we classify each paper and then analyze advantages and limitations to analyze which methods are suitable to be implemented in the Wireless Ad hoc Networks application in IoT.

SYBIL ATTACK PROPERTIES

Sybil attack is defined as an intrusion, where malicious devices get or change into several different identities illegally. Newsome conveys the impact of the Sybil attack on several protocols, including the following:

Distributed storage: when there are nodes that cannot provide services, then the node will share its data to neighboring nodes. If this neighbor node is a Sybil node, then the data can be obtained.

Routing: especially a network that has a sink, when the Sybil point has gained control of the sink node, in addition to the Sybil node getting all data passed on the network, many other attacks can be carried out.

Data aggregation: if the Sybil node mediates data packets, then it can manipulate the data.

Voting: by increasing the number of nodes, Sybil nodes can influence the results of the voting, or a majority of Sybil points can accuse legitimate points of being evil.

Fair allocation of resources: the Sybil node can disrupt the system by unauthorized activation/deactivation of the node. So as to avoid these impacts, defense machineries that can accurately detect Sybil attacks are needed. To be able to design these defense machineries, knowledge is needed to recognize behavior and predict the possible actions of the Sybil attacker. Mishra (Mishra AK et al., 2019) classifies Sybil attacks based on nature and tasks carried out during this attack into three phases, namely, the compromise, deployment, and launch phases.

Compromised phase

The attacker tries to get a group of nodes that can be controlled by the attacker. There are two characteristics of Sybil attack at this stage, according to the way the attacker gets a node to be able to enter the network, namely, stealing/compromise and fabrication. This phase ends when the attacker gets a group of compromised nodes that are connected in the destination network.

- Fabrication: characteristics of Sybil attacks with Fabrication are usually carried out when there is the possibility of the attacker to create a new identity in accordance with network requirements. For example, if the network only gives an ID in the form of a number of n-bits, the Sybil attacker can create a new random identity randomly within a valid range (0 to n) so that it is recognized as a valid node.
- Stealing/compromise: if a fabrication attack cannot be carried out, then what the attacker can do is to steal the identity of a valid node. If one of the nodes or a group of valid nodes in the network can be taken over, the attacker can use this node directly, or by taking its identity, then the attacker temporarily interferes with the valid node or destroys it permanently.

Deployment phase

Sybil attackers will try to spread the nodes that are taken over by gathering network-related information. The most crucial thing in this phase is that the attacker will determine the placement of compromised nodes in strategic locations and allow for success in the launch phase. Sybil nodes can be moved at specific locations to be able to attack simultaneously, or individual nodes can be endeavored to take on the role of cluster heads.

There are two characteristics of Sybil at this stage, according to the capabilities of the Sybil attacker, namely, by spreading randomly and selectively.

- Random Deployment: the attacker chooses a location to use Sybil randomly.
- Selective Deployment: the attacker selectively chooses the set of Sybil nodes it has, for example, deploying the group at one central location so that it can dominate that location, or the attacker can spread Sybil nodes to various places on the network to avoid behavior-based detection.

Launching phase

There are several forms of Sybil attacks in carrying out attacks. This is adjusted to the objectives to be achieved by the attack, whether to disrupt the system, do the DoS, or other objectives. Forms of attack that are launched are also usually intended to avoid detection systems. The attack can be carried out directly, i.e., the Sybil node communicates directly with the valid node, or indirectly, i.e., the attack is carried out by communication through one of the Sybil nodes.

Indirect Communication in this attack version is when there is no node that can communicate directly with Sybil. Instead, one or more malicious devices are claimed to have reached Sybil's point. Messages sent to the Sybil node are routed through one of these dangerous intersections, which pretends that the message is returned to the Sybil node.

- Simultaneous attackers deploy a group or all Sybil nodes simultaneously. This group can directly connect with the network or participate through other Sybil points.
- Nonsimultaneous attackers do not attack simultaneously; for example, the attacker can choose attacks alternately according to a specific time lag. Usually, this is done to avoid specific detection.
- Conspiracy Sybil is Sybil attacks that conspire to do so by attacking the Sybil Node network that will freely control nodes that are compromised by other points as accomplices to attack directly or by using these nodes to give new identities to other Sybil nodes. The Sybil conspiracy attack in Vehicle Ad hoc Network (VANET) was first introduced in Feng X et al. (2017), where the attacker could pretend to be a conspiracy node, and then his identity is to send malicious messages to other nodes nearby.

SYBIL DETECTION IN WIRELESS AD HOC NETWORK

Table 1. Sybil Defense Mechanism in WANET Taxonomy.

Method	Schemes		Reference
Cryptography Based	Authentication Based	Password Comparison Zero-Knowledge Protocol Fujisaki-Okamoto	Amuthavalli R et al., 2014
		GSM's SRES	Saud Khan M et al., 2016
	Public Key Infrastructure	ID-based Signature	Vinayagam SS et al., 2014
		Certificate trust	
		Pseudo Certificate	
		Token-Based	
		Group Signature	
	Watermarking Based		Harjito B et al., 2017
	Symmetric key Based		Aggarwal P et al., 2015, Ambika N et al., 2014
Location Based	RSSI Based	Observer collection	De Sales TM et al., 2014, Li M, Xiong Y et al., 2013, Jan MA et al., 2015
		Neighbor Collection	Liu R et al., 2014, Jan MA et al., 2018, Demirbas M et al., 2006, Wang J et al., 2008, Bhuvaneshwari G et al., 2014, Lv S et al., 2008, Faisal M et al., 2018, Yao Y et al., 2019
	Time-based	ToA / TDoA	Huang X et al., 2012, Garg N et al., 2014, Rajesh M et al., 2012
		TDMA Spider Monkey	Ali Alheeti KM et al., 2018, Iwendi C et al., 2018
		Time Synchronization	Wang Z et al., 2018, Dong W et al., 2015, Benzaid C et al., 2011
	Range free		Geetha C et al., 2015, Shi W et al., 2015, Ayaida M et al., 2019, Patil DS et al., 2017, Grover J et al., 2010, Karuppiah AB et al., 2014, Tian B et al., 2013
Network Feature/ Behavior	Traffic and Mobility		Han S et al., 2017, Golestani Najafabadi S et al., 2013
	Enter - Exit Behavior Attack Edge		Jamshidi M et al., 2018, Silawan T et al., 2016
	Node relation (Graph)		Subba B et al., 2018, Zhang K et al., 2014, Sicari S et al., 2017
	Network/physical data		Singh R et al., 2017, Sujatha V et al., 2017, Wang H et al., 2018, Gantsou D et al., 2015
Resource Test	Energy-Based	Power Signal Strength Clock Skew State Information Speed info Transient based Radio Fingerprinting MAC and MAP	Gaikwad V et al., 2017, Sinha S. et al., 2013, Saggi MK et al., 2015, Danev B et al., 2009, Uddin MB et al., 2011, Sieka B et al., 2006, Lakhanpal R et al., 2016
	Physical Fingerprinting		
Trust-Based	Centralized trust	Game-Based	Liao X et al., 2011, Tanuja R et al., 2012, Jamshidi M et al., 2017, Hsieh C et al., 2011
		Reputation Based	
		Bayes rule filter	
		Energy cost	Hamdan S et al., 2018, Nikam A et al., 2018, Meena Kowshalya A et al., 2016, Edwin Prem Kumar G et al., 2016, Triki B et al., 2014
		Routing based	
		Ant colony	
		Physical trust	
	Decentralized trust (neighbor trust)	Position Based	Tang Q et al., 2018, Wang W-T et al., 2010, Ssu K-F et al., 2009
		Sequential Hypothesis testing	Vamsi PR et al., 2014
		Message Exchange	Shi Y-L et al., 2018, Chen C et al., 2011, Grover J et al., 2014
		Ultra-wideband ranging	Sarigiannidis P et al., 2015
		Speed	Medjek F et al., 2017

The defense mechanism of Sybil by considering the characteristics of Sybil that has been mentioned is vital to improve detection accuracy. We have reviewed several defense machineries from Sybil attacks on Wireless Ad Hoc Networks using the Systematic Literature Review (SLR) method. In general, the steps taken are planning, implementation, and documentation. The planning step consists of identifying review needs, defining and taking specific research questions, developing research protocols, and evaluating review protocols. In the second stage, the implementation of research identification is carried out by conducting a pilot selection and extraction, followed by a selection of the main study quality assessment, data extraction, and data synthesis. The last step taken is documentation, including drawing conclusions and considering threats.

The basic research question in this Systematic Literature Review (SLR) is "what methods are used in defense machinery against Sybil attacks?" to get an overview of the development of forms of security against Sybil in Wireless Ad hoc Networks. The next step, for the search strategy, we use several digital libraries with the search string '(SYBIL ATTACK) AND DETECTION AND ("WIRELESS AD-HOC NETWORKS" OR "MOBILE AD-HOC NETWORKS" OR "VEHICLE AD-HOC NETWORK")'. Then, according to the research question, the primary study is grouped into a taxonomy as seen in Table 1. After obtaining a group of methods used in the defense mechanism against Sybil attacks, a weakness analysis is carried out on each defense mechanism for its application to IoT.

Cryptographic based

This method uses the cryptographic protocol often found mainly to prevent the occurrence of Sybil attacks. Broadly speaking, this defense mechanism is performed by authenticating nodes, using public key certificates to guarantee trust, using secret symmetric keys to prevent other nodes from communicating with the network, and using watermarking to guarantee valid data.

Authentication: the schema working with each node must be able to prove that it is a valid node through a series of message exchanges on the authentication protocol.

Public Key Infrastructure: a cryptographic system based on public keys is used to improve security by allowing nodes to communicate in networks with trust values based on certificates held. In this system, certificate-based techniques are used in encryption and authentication machinery. Centralized authority for certification is required.

Symmetric key: this scheme relies on encrypting and decrypting messages between nodes using a symmetric encryption algorithm. This technique is used in the network to create secure paths to communicate with each other by using a set of preagreed keys or using a trusted third party to ensure the distribution of keys to all legitimate nodes in the network. With this defense mechanism, the Sybil node will have difficulty getting the key so that it is only possible to obtain a compromised node by stealing.

Watermarking: Watermarking techniques are used to be the solution to implementing cryptography on devices with limited resources. The main idea is to embed information that allows an individual to add verification messages to communication data. So, the Sybil nodes cannot make an attack because it cannot change the watermark constraints that have been embedded in the data.

The application of IoT defense machinery using cryptography has the following disadvantages:

a. Dependence on cryptographic hardware and software.

b. Compatibility issue with network types and routing protocols on IoT.

c. Scalability in the addition of new nodes/points that may increase resource requirements exponentially.

d. High memory, computing, and communication overhead that is not suitable for resource constraints network.

e. To ensure the network has safe keys and algorithms and high costs are needed for key generation and key distribution

Location verification based

a. The location-/position-based method utilizes measurement parameters that can be physically observed to estimate the location and position of the node to detect Sybil attacks. This method is used with the assumption that there may not be different nodes that are in the same location. So, if found, it will be concluded as a Sybil node. Another assumption is to use position verification, where a node equipped with a Global Positioning System (GPS) will send its location to a valid node, and then the node will verify based on the estimated position of the propagation model of the received signal.

b. As stated in Zhang T et al. (2012), this method can be grouped into two categories, namely, range-based and range-free methods.

c. Range-based: the estimated position is calculated based on the physical indicator used to estimate the distance between the transmitter and receiver. This distance estimate is usually based on the Received Signal Strength Indicator (RSSI), time-based methods such as Time of Arrival (ToA) and Time Difference of Arrival (TDoA). This method is suitable for IoT devices because it is low in cost, where the distance between two entities is estimated only based on the received signal strength and the indicators the device has by default.

d. Range-free method has high accuracy in distance calculation. By utilizing data from GPS, Radar, or location-based/localization scheme, this method can also be used as a support for position estimation using ranged based.

e. Applying IoT, the location-/position-based defense method has the following disadvantages:

f. It is not suitable for use on mobile networks such as MANET and VANET, and the accuracy of approximate location decreases due to rapid changes in network topology and changes in node position.

g. The accuracy of the method depends on the environment. Interference, multipath fading, and shadowing lead to inaccurate location estimation.

h. This method is not enough if implemented as a single mechanism. It will be challenging to detect nodes that can manipulate signal strength or decrypt conspiring nodes.

i. With the increase in node density, it is possible when two or more honest nodes that have adjacent positions are identified as Sybil nodes.

j. There are possible privacy violations, where identity is required to send position information so that the route of movement of the nodes can be traced.

Behavior-based network

This method purely detects Sybil nodes based on their features and behavior in the network. The detection method specifically detects features that allow accurate classification between Sybil nodes and valid nodes.

In applying IoT, network behavior-based defense method has the following disadvantages:

a. It only detects Sybil nodes according to the context expected by the detection method, so that Sybil nodes with specific knowledge can escape detection.

b. It requires specialized hardware that has a large capacity to collect and analyze data.

Resource testing

By testing the unique resources of the node, assuming that each physical node has specific limited resources, a node will be challenged to provide knowledge about specific resources (usually in the form of physical fingerprinting or based on energy), and then the verifier compares the resources used by an entity with the typical value or threshold of the resources owned by that entity. Incompatibility indicates the possibility of a Sybil attack.

Energy-based: the basic idea of energy-based testing is to verify the assumption that the node has a predictable energy parameter, so that if a node is found to be incompatible with the existing node in providing an answer, then the node is considered a malicious node.

Physical fingerprinting: each device has unique characteristics. These characteristics are the basis of verification to determine whether the point is valid or not.

In applying IoT, the resource testing defense method has some disadvantages including:

a. Exponential increase for each node addition.

b. Extensive power consumption due to the need to carry out testing at all times.

c. Assuming a single channel, attackers who have more than one channel can manipulate the results of resource testing.

d. Valid nodes that have resource problems due to DoS or conditions such as power blackouts, overloaded processors, and others can be considered Sybil nodes.

Trust-based

Trust is defined as a relationship of trustor and trustee; the trustor can periodically evaluate the trusteeship to assess its eligibility. Trusted-based method is based on the value of trust that must be maintained by each node to remain in the network. This trust value can be obtained from trusted devices or from neighbor trusts.

Centralized trust: In the trust-based method, using a trusted device, usually in the initial stage, a comprehensive network mapping is carried out on all nodes, with the device obtaining its identity and trust value. Then, the trust value is evaluated to determine the possibility that the node is not a Sybil node.

Decentralized trust: In the detection approach based on the relationship between neighbors, each node will visit nearby nodes based on the pattern of relationships and behavior of these nodes in the network.

In applying IoT, the trust-based defense method has some disadvantages including the fact that the method will not be able to detect if Sybil node dominates the number of nodes in the process of determining the value of trust.

The defense mechanism of Sybil by considering the characteristics of Sybil that has been mentioned is essential to improve detection accuracy. From the reviewed papers, we select several latest proposed schemes to present how each method can be used to recognize properties of Sybil attack in every phase in Table 2. As shown in the table, not all defense machinery can handle all Sybil attack properties; some have implemented privacy protections, and some can work on mobile networks and fast-changing networks. A practical, energy-efficient, versatile defense mechanism that can cover all Sybil attacks properties is highly recommended.

Table 2. Comparison of defense machinery against the properties of Sybil attacks.

References	Method	Scheme	Privacy	Static/ Mobile	Structure	Sybli Attack Properties						
						C1	C2	D1	D2	L1	L2	L3
Nirmal Raja K et al., 2017	Authentication	Authenticate node by Fujisaki-Okamoto scheme	no	mobile	centralized	√	√	√	-	√	√	-
Feng X et al., 2017	PKI based	ID Obfuscated and Publik key certificate	yes	mobile	centralized	√	-	√	-	√	√	-
Sharma AK et al., 2016	PKI based	Data protection via Public Key Encryption	no	mobile	centralized	√	√	√	-	√	-	-

Harjito B et al., 2017	Watermarking	Data Validation by Kolgomorov	no	mobile	decentralized	√	-	√	√	√	√	-
V et al., 2017	Symmetric key	Network data protection by symetric encryption	yes	mobile	centralized	√	-	√	√	√	√	-
Yuan Y et al., 2018	RSSI based	Range Free using APIT Localization	no	static	decentralized	√	√	√	-	√	-	-
Yao Y et al., 2019	RSSI Based	voiceprint based on RSSI	no	Mobile	decentralized	√	√	√	-	√	-	√
Selvakumar K et al., 2019	Time Based	Node-identification-based secure time synchronization	no	static	decentralized	√	-	√	√	√	-	-
Iwendi C et al., 2018	Time Based	prediction in a challenge zone using Spider monkey technique	no	mobile	Centralized	√	√	√	√	√	-	√
Ayaida M et al., 2019	Range-free	Based on the macroscopic traffic flow theory to detect Sybil attacks	no	mobile	decentralized	√	-	√	-	√	√	-
Abbas S et al., 2019	Range-free	A distributive algorithm based on RSSI and collaboration of cluster head nodes	no	static	centralized	√	-	√	√	√	√	-
Silawan T et al., 2016	Net Feature	persuading function with assumption attack edge is more than mistaken edge	no	static	decentralized	√	√	√	-	√	√	√
Singh R et al., 2017	Net Feature	based on fuzzy rule sets along with the Multilayer Perceptron Neural Network	no	static	centralized	√	-	√	√	√	√	-
Li Q, et al., 2019	Energy Based	based on power gain and delay spread exacted from receiving packets	no	static	decentralized	-	√	√	-	√	-	√
Wang C et al., 2018	Energy Based	based on Channel State Information	no	mobile	decentralized	√	√	√	√	√	√	-
Jamshidi M et al., 2017	Central Trust	Use Watchdog Nodes to label mobile nodes based on their movement behaviors	no	mobile	centralized	√	-	√	√	√	√	√
Airehrour D et al., 2019	Central Trust	uses a trust-based mechanism in RPL routing protocol	no	static	centralized	√	√	√	√	√	√	-
V et al., 2010	Neighbor Trust	based on number allocating and mutual guarantee relying on neighbors	no	mobile	decentralized	-	√	√	√	√	√	√
Sarigiannidis P et al., 2015	Neighbor Trust	uses rule-based anomaly detection system relies on UWB ranging-based info	no	static	decentralized	√	√	√	√	√	-	√

DISCUSSION

General detection issue

As a general need for defense machinery in the Wireless Ad hoc network to be integrated with IoT, several issues related to the accuracy of defense machinery, the possibility of implementation, and others arise; some issues related to this include the following:

Accuracy: defense mechanism can detect Sybil at each phase with different properties. It must be able to discover a large percentage of Sybil nodes to eliminate damage.

Cooperative Sybil detection: to detect effectively, all nodes in the network participate independently in the Sybil node detection process.

Low overhead costs: the proposed approach works more efficiently and requires fewer system resources.

a. Does not need additional hardware at high prices.

b. Does not increase message exchange on the network.

c. Does not require much memory.

Detection time: the time needed to find and delete a Sybil entity is an essential factor that must be minimal.

Implementation: for every IoT implementation such as in Industry, Smarthome, and Smart grid, there are special needs that must be considered in applying defense machinery.

Vanet issue

In the wireless ad hoc network area, VANET has become the most talked about topic lately, with specific needs that VANETs require additional requirements for security guarantees. Issues discussed in several papers reviewed are as follows:

Privacy Issue: most vehicle users hope that their identity information can be stored in VANET because they are afraid that their trip will leak with that identity.

Safety Issue: VANET does not allow a decrease in reputation after a severe traffic accident to prevent another attack, because damage to life and things in this attack cannot be repaired.

Learning-based issue

Defense machinery in the IoT infrastructure must be prepared with the needs of a "smart" system so that the application of scientific fields on artificial intelligence, especially machine learning, is extremely open. Several machine learning methods have succeeded in detecting specific attacks on IoT (L. Xiao et al., 2018). Machine learning methods that need to be applied to Sybil's defense machinery include the following:

Deep Learning: with the development and the number of entities in an IoT infrastructure, a mechanism based on thorough analysis is needed; deep learning has been successfully used in various areas including intrusion detection systems.

Transfer Learning: with regard to data that is continuously changing, and the possibility of attacks at an advanced level, this requires a defense machinery that can prevent even new types of Sybil attacks.

Online Learning: most of the data sent on IoT infrastructure, including WANET-based IoT, are data stream, so online learning needs to be a concern for solutions on detection that continuously enhance the capability of defense machinery.

Centralized vs. decentralized issue

Centralized issue: some defense machineries use centralized detection, which requires a trusted center. Several papers on VANET build trust relationships that are bestowed on RSU. Installation of such infrastructure nationally is challenging to achieve in the early stages of VANET. Even in the medium term, there may still be many places that are not covered by RSU.

Decentralized issue: on the mechanism that relies on each node as a detector, all must know the credibility of each node that shares information around it and ensure that all messages received are trusted and correct. However, this mechanism can work well assuming that most nodes are trusted nodes.

CONCLUSION

In this paper, we have provided a comprehensive review of defense machinery against Sybil attacks, including defining the Sybil attack properties, building the taxonomy of these machinery, and analyzing the problems that still exist in defense machinery against Sybil on Wireless Ad hoc Networks related to their implementation in IoT. Several defense machineries have been proposed for Sybil attacks on WANET, which are mostly based on cryptography, location or position, network behavior, resource testing, and trust. However, the drawbacks are that not all machineries are suitable for use in networks with limited resources. This paper presents a survey, classification, and comparison of various defense machineries that have been proposed for non-IoT WANETs. Several challenges have been mentioned to be implemented in a practical IoT system. We hope that this survey will provide readers with the big picture and current knowledge related to this topic.

REFERENCES

Abbas S. 2019. An efficient sybil attack detection for internet of things. Advances in Intelligent Systems and Computing. 2019; **931**: 339-49.

Abdulkader ZA, Abdullah A, Abdullah MT & Zukarnain ZA. 2018. A survey on sybil attack detection in vehicular ad hoc networks (VANET). Journal of Computers (Taiwan). 2018; **29**(2): 1-6.

Aggarwal P & Rai MK. 2015. A novel scheme for detection of selective forwarding attack and sybil attack in wireless sensor network. International Journal of Applied Engineering Research. 2015; **10**(10): 25929-38.

Airehrour D, Gutierrez JA & Ray SK. 2019. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems. 2019; **93**: 860-76.

Ali Alheeti KM, Al-ani MS & McDonald-Maier K. 2018. A hierarchical detection method in external communication for self-driving vehicles based on TDMA. PLoS ONE. 2018; **13**(1).

Amuthavalli R & Bhuvaneswaran RS. 2014. Detection and prevention of Sybil attack in wireless sensor network employing random password comparison method. Journal of Theoretical and Applied Information Technology. 2014; **67**(1): 236-46.

Ambika N & Raju GT. 2014. ECAWSN: Eliminating compromised node with the help of auxiliary nodes in wireless sensor network. International Journal of Security and Networks. 2014; **9**(2): 78-84.

Ayaida M, Messai N, Najeh S & Ndjore KB. 2019. A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs. Ad Hoc Networks. 2019;101845.

Benzaid C, Saiah A & Badache N. 2011. Secure pairwise broadcast time synchronization in wireless sensor networks. In: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS). 2011. p. 1-6.

Bhuvaneshwari G & Udayakumar R. 2014. Detecting the identities of sybil attack in manet based on Rss detection. International Journal of Applied Engineering Research. 2014; **9**(22): 7251-4.

Chen C, Han W & Wang X. 2011. Sybil attack detection based on signature vectors in VANETs. International Journal of Critical Computer-Based Systems. 2011; **2**(1): 25-37.

Danev B & Capkun S. 2009. Transient-based Identification of Wireless Sensor Nodes. In: Proceedings of the 2009 International

Conference on Information Processing in Sensor Networks. Washington, DC, USA: IEEE Computer Society; 2009. p. 25-36. (IPSN '09). 0

Demirbas M & Song Y. 2006. An RSSI-based scheme for sybil attack detection in wireless sensor networks. In: Proceedings - WoWMoM 2006: 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2006. p. 564-8.

De Sales TM, Almeida HO, Perkusich A, De Sales L & De Sales M. 2014. A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks. In: Digest of Technical Papers - IEEE International Conference on Consumer Electronics. 426-7.

Dong W & Liu X. 2015. Robust and Secure Time-Synchronization Against Sybil Attacks for Sensor Networks. IEEE Transactions on Industrial Informatics. 2015 Dec; **11**(6): 1482-91.

Edwin Prem Kumar G, Baskaran K, Elijah Blessing R & Lydia M. 2016. Evaluation of hybrid trust models using ant colony optimization in wireless sensor networks. International Journal on Smart Sensing and Intelligent Systems. 2016; **9**(3): 1243-60.

Faisal M, Abbas S & Ur Rahman H. 2018. Identity attack detection system for 802.11-based ad hoc networks. Eurasip Journal on Wireless Communications and Networking. 2018; **2018**(1).

Feng X, Li C, Chen D & Tang J. 2017. A method for defensing against multi-source Sybil attacks in VANET. Peer-to-Peer Networking and Applications. 2017 Mar; **10**(2): 305-314.

Feng X & Tang J. 2017. Obfuscated RSUs Vector Based Signature Scheme for Detecting Conspiracy Sybil Attack in VANETs. Mobile Information Systems. 2017; 2017.

Gaikwad V & Ragha L. 2017. Mitigation of attack on authenticating identities in ad-hoc network. In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). 2017. p. 1027-32.

Gantsou D. 2015. On the use of security analytics for attack detection in vehicular ad hoc networks. In: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings. 2015.

Garg N, Pareek K, Gaur MS, Laxmi V & Lal C. 2014. Analysis of Identity Forging Attack in MANETs. In: Proceedings of the 7th International Conference on Security of Information and Networks. New York, NY, USA: ACM; 2014. p. 441: 441-441:446. (SIN '14).

Geetha C & Ramakrishnan M. 2015. A hybrid scheme for detecting clone and Sybil attacks in wireless sensor networks. International Journal of Applied Engineering Research. 2015; **10**(9): 22467-76.

Golestani Najafabadi S, Naji HR & Mahani A. 2013. Sybil attack Detection: Improving security of WSNs for smart power grid application. In: Smart Grid Conference 2013, SGC 2013. 2013. p. 273-8.

Grover J, Gaur MS & Laxmi V. 2010. A Novel Defense Mechanism Against Sybil Attacks in VANET. In: Proceedings of the 3rd International Conference on Security of Information and Networks. New York, NY, USA: ACM; 2010. p. 249–255. (SIN '10). Available from: http://doi.acm.org/10.1145/1854099.1854150

Grover J, Laxmi V & Gaur MS. 2014. Sybil attack detection in VANET using neighbouring vehicles. International Journal of Security and Networks. 2014; **9**(4): 222-33.

Han S, Ban D, Park W & Gerla M. 2017. Localization of Sybil Nodes with Electro-Acoustic Positioning in VANETs. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference. 2017. p. 1-6.

Harjito B. 2017. Kolmogorov watermarking technique for secure the data of Wireless Sensor Networks. In: 2017 Second International Conference on Informatics and Computing (ICIC). 2017. p. 1-6.

Hamdan S, Hudaib A & Awajan A. 2018. Hybrid Algorithm to Detect the Sybil Attacks in VANET. In: 2018 FIFTH INTERNATIONAL SYMPOSIUM ON INNOVATION IN INFORMATION AND COMMUNICATION TECHNOLOGY (ISIICT 2018). Amity Univ; IEEE, Jordan Sect; 2018. p. 93-8.

Hsieh C, Huang Y & Chen R. 2011. A Light-Weight Ranger Intrusion Detection System on Wireless Sensor Networks. In: 2011 Fifth International Conference on Genetic and Evolutionary Computing. 2011. p. 49-52.

Huang X, Ahmed MR & Sharma D. 2012. A novel protection for wireless sensor networks from internal attacks. In: Lecture Notes in Engineering and Computer Science. p. 374-9.

Iwendi C, Uddin M, Ansere JA, Nkurunziza P, Anajemba JH & Bashir AK. 2018. On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique. IEEE Access. 2018; **6**: 47258-67.

Jan MA, Nanda P, He X & Liu RP. 2015. A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network. In: 2015 IEEE TRUSTCOM/BIGDATASE/ISPA, VOL 1. IEEE; IEEE COMP SOC; IEEE Tech Comm Scalable Comp; Aalto Univ, Sch Elect Engn; Integrated Serv Networks, State Key Lab; NOKIA; SSH; ERICSSON; Tekes; Federat Finnish Learned Soc; Xidian Univ; 2015. p. 318-25.

Jamshidi M, Zangeneh E, Esnaashari M & Meybodi MR. 2017. A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks. COMPUTERS & ELECTRICAL ENGINEERING. 2017 Nov; **64**: 220-32.

Jamshidi M, Darwesh AM, Lorenc A, Ranjbari M & Meybodi MR. 2018. A precise algorithm for detecting malicious sybil nodes in mobile wireless sensor networks. IEIE Transactions on Smart Processing and Computing. 2018; **7**(6): 457-66.

Karuppiah AB, Dalfiah J, Yuvashri K, Rajaram S & Pathan A-SK. 2014. A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks. In: Chandrasekaran, K and Tahiliani, MP and Mathew, J, editor. 2014 3RD INTERNATIONAL CONFERENCE ON ECO-FRIENDLY COMPUTING AND COMMUNICATION SYSTEMS (ICECCS 2014). Natl Inst Technol,Dept Comp Sci & Engn; IEEE; IEEE Comp Soc; 2014. p. 95-8.

Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J & Linkman S. Systematic Literature Reviews in Software Engineering - A Systematic Literature Review. Inf Softw Technol. 2009 Jan; **51**(1): 7-15.

L. Xiao, X. Wan, X. Lu, Y. Zhang & D. Wu. 2018. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Processing Magazine. 2018 Sep; **35**(5): 41-9.

Lakhanpal R & Sharma S. 2016. Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique. In: 2016 International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC 2016. 2016. p. 283-7.

Liao X, Hao D & Sakurai K. 2011. Achieving cooperative detection against Sybil attack in wireless ad hoc networks: A game theoretic approach. In: 17th Asia-Pacific Conference on Communications, APCC 2011. 2011. p. 806-11.

Li Q & Cheffena M. 2019. Exploiting Dispersive Power Gain and Delay Spread for Sybil Detection in Industrial WSNs: A Multi-Kernel Approach. IEEE Transactions on Wireless Communications. 2019 Mar; **18**(3): 1805-18.

Li M, Xiong Y, Wu X, Zhou X, Sun Y, Chen S, et al. 2013. A Regional Statistics Detection Scheme against Sybil Attacks in WSNs. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. 2013. p. 285-91.

Liu R & Wang Y. 2014. A New Sybil Attack Detection for Wireless Body Sensor Network. In: 2014 Tenth International Conference on Computational Intelligence and Security. 2014. p. 367-70.

Lv S, Wang X, Zhao X & Zhou X. 2008. Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks. In: 2008 International Conference on Computational Intelligence and Security. 2008. p. 442-6.

Lu Tan & Neng Wang. 2010. Future internet: The Internet of Things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). 2010. p. V5-376.

Medjek F, Tandjaoui D, Romdhani I & Djedjig N. 2017. Performance Evaluation of RPL Protocol under Mobile Sybil Attacks. In: 2017 IEEE Trustcom/BigDataSE/ICESS. 2017. p. 1049-55.

Meena Kowshalya A & Valarmathi ML. 2016. Detection of Sybil's across communities over Social Internet of Things. Journal of Applied Engineering Science. 2016; **14**(1): 75-83.

Mishra AK, Tripathy AK, Puthal D & Yang LT. 2019. Analytical Model for Sybil Attack Phases in Internet of Things. IEEE INTERNET OF THINGS JOURNAL. 2019 Feb; **6**(1, SI): 379-87.

Nikam A & Ambawade D. 2018. Opinion Metric Based Intrusion Detection Mechanism for RPL Protocol in IoT. In: 2018 3rd International Conference for Convergence in Technology (I2CT). 2018. p. 1-6.

Nirmal Raja K & Maraline Beno M. 2017. Secure Data Aggregation in Wireless Sensor Network-Fujisaki Okamoto(FO) Authentication Scheme against Sybil Attack. Journal of Medical Systems. 2017; **41**(7).

Newsome J, Shi E, Song D & Perrig A. 2004. The Sybil Attack in Sensor Networks: Analysis & Defenses. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks. New York, NY, USA: ACM; 2004.

p. 259-268. (IPSN '04).

Parikh N & Das ML. 2017. Privacy-preserving services in VANET with misbehavior detection. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). 2017. p. 1-6.

Patil DS & Patil SC. 2017. A Novel Algorithm for Detecting Node Clone Attack in Wireless Sensor Networks. In: 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). 2017. p. 1-4.

Rajesh M, Gangadev GR & Sugavanam R. 2012. On Recognizing ID Based Attacks Using Environs and Beam forming Approach for Wireless Sensor Networks. In: 2012 THIRD INTERNATIONAL CONFERENCE ON COMPUTING COMMUNICATION & NETWORKING TECHNOLOGIES (ICCCNT). 2012. (International Conference on Computing Communication and Network Technologies).

Reina DG, Toral SL, Barrero F, Bessis N & Asimakopoulou E. 2019. The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments. In: Bessis N, Xhafa F, Varvarigou D, Hill R, Li M, editors. Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. Berlin, Heidelberg: Springer Berlin Heidelberg; 2013 [cited 2019 Aug 17]. p. 89-113. (Studies in Computational Intelligence).

Saggi MK & Kaur R. 2015. Isolation of Sybil attack in VANET using neighboring information. In: 2015 IEEE International Advance Computing Conference (IACC). 2015. p. 46-51.

Sarigiannidis P & Karapistoli E. 2015. Economides AA. Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. Expert Systems with Applications. 2015; **42**(21):7560-72.

Saud Khan M & Khan NM. 2016. Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks. Journal of Sensors. 2016; 2016.

Sharma AK, Saroj SK, Chauhan SK & Saini SK. 2016. Sybil Attack Prevention and Detection in Vehicular Ad hoc Network. In: Astya, PN and Swaroop, A and Sharma, V and Singh, M, editor. 2016 IEEE INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND AUTOMATION (ICCCA). IEEE; IEEE UP Sect; IEEE Uttar Pradesh Sect SP C Chapter; Galgotias Univ, Sch Comp Sci & Engn; 2016. p. 594-9.

Shi Y-L & Wang L-M. 2018. Spatio-Temporal Analysis Based Resist Conspiracy Sybil Attack Detection in VANETs [VANETs中基于时空分析的抗合谋Sybil攻击检测方法]. Jisuanji Xuebao/Chinese Journal of Computers. 2018; **41**(9): 2148-61.

Selvakumar K & Naveen Kumar S. 2019. Security issues and ANALYSING sybil attack detection in VANET. International Journal of Recent Technology and Engineering. 2019; **7**(5):386-91.

Sicari S, Rizzardi A & Grieco LA. 2017. Coen-Porisini A. Performance comparison of reputation assessment techniques based on self-organizing maps in wireless sensor networks. Wireless Communications and Mobile Computing. 2017; 2017.

Singh R, Singh J & Singh R. 2017. Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. Wireless Communications and Mobile Computing. 2017; 2017.

Shi W, Liu S & Zhang Z. A. 2015. Lightweight Detection Mechanism against Sybil Attack in Wireless Sensor Network. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS. 2015 Sep 30; **9**(9): 3738-50.

Sieka B. 2006. Using radio device fingerprinting for the detection of impersonation and Sybil attacks in wireless networks. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2006;4357 LNCS:179-92.

Silawan T & Aswakul C. 2016. SybilComm: Sybil community detection using persuading function in IoT system. In: 2016 International Conference on Electronics, Information, and Communications (ICEIC). 2016. p. 1-4.

Sinha S, Paul A & Pal S. 2013. The sybil attack in Mobile Adhoc Network: Analysis and detection. In: Third International Conference on Computational Intelligence and Information Technology (CIIT 2013). 2013. p. 458-66.

Subba B, Biswas S & Karmakar S. 2018. A game theory based multi layered intrusion detection framework for VANET. Future Generation Computer Systems. 2018; **82**:12-28.

Sujatha V & Mary Anita EA. 2017. Fuzzy based scheme for detection of Sybil node in wireless sensor networks. Journal of Advanced Research in Dynamical and Control Systems. 2017; 9(Special Issue 6): 815-22.

Ssu K-F, Wang W-T & Chang W-C. 2009. Detecting Sybil attacks in Wireless Sensor Networks using neighboring information. Computer Networks. 2009; **53**(18): 3042-56.

Tang Q & Wang J. 2018. A secure positioning algorithm against Sybil attack in wireless sensor networks based on number allocating. In: International Conference on Communication Technology Proceedings, ICCT. 2018. p. 932-6.

Tanuja R, Anoosha V, Manjula SH, Venugopal KR, Iyengar SS & Patnaik LM. 2012. Secure reputation update for target localization in wireless sensor networks. Communications in Computer and Information Science. 2012;292 CCIS:109-18.

Tian B, Yao Y, Shi L, Shao S, Liu Z & Xu C. 2013. A novel sybil attack detection scheme for wireless sensor network. In: 2013 5th IEEE International Conference on Broadband Network Multimedia Technology. 2013. p. 294-7.

Triki B, Rekhis S & Boudriga N. 2014. An RFID based System for the detection of Sybil attack in Military Wireless Sensor networks. In: 2014 World Congress on Computer Applications and Information Systems (WCCAIS). 2014. p. 1-2.

Uddin MB & Castelluccia C. 2019. Towards clock skew based services in wireless sensor networks. International Journal of Sensor Networks. 2011; **9**(1): 24-37.

Vamsi PR & Kant K. 2014. Sybil attack detection using Sequential Hypothesis Testing in Wireless Sensor Networks. In: 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014). 2014. p. 698-702.

Vasudeva A & Sood M. 2018. Survey on sybil attack defense machinery in wireless ad hoc networks. JOURNAL OF NETWORK AND COMPUTER APPLICATIONS. 2018 Oct 15; **120**: 78-118.

Vinayagam SS & Parthasarathy V. 2014. IPTTA: Leveraging Token-Based Node IP Assignment and Verification for WSN. In: 2014 International Conference on Science Engineering and Management Research (ICSEMR).

Wang C, Zhu L, Gong L, Zhao Z, Yang L, Liu Z, et al. 2018. Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information. SENSORS. 2018 Mar; **18**(3).

Wang H, Wen Y & Zhao D. 2018. Identifying localization attacks in wireless sensor networks using deep learning. Journal of Intelligent and Fuzzy Systems. 2018; **35**(2): 1339-51.

Wang J, Yang G, Sun Y & Chen S. 2008. Defending against Sybil attacks based on received signal strength in wireless sensor networks. Chinese Journal of Electronics. 2008; **17**(4): 611-614.

Wang W-T, Ssu K-F & Chang W-C. 2010. Defending Sybil attacks based on neighboring relations in wireless sensor networks. Security and Communication Networks. 2010; **3**(5): 408-20.

Wang Z, Zeng P, Kong L, Li D & Jin X. 2018. Node-identification-based secure time synchronization in industrial wireless sensor networks. Sensors (Switzerland). 2018; **18**(8).

Yao Y, Xiao B, Wu G, Liu X, Yu Z, Zhang K, et al. 2019. Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI. IEEE Transactions on Mobile Computing. 2019 Feb; **18**(2): 362-75.

Yuan Y, Huo L, Wang Z & Hogrefe D. 2018. Secure APIT Localization Scheme Against Sybil Attacks in Distributed Wireless Sensor Networks. IEEE Access. 2018; **6**: 27629-36.

Zhang K, Liang X, Lu R & Shen X. 2014. Sybil Attacks and Their Defenses in the Internet of Things. IEEE INTERNET OF THINGS JOURNAL. 2014 Oct; 1(5, SI): 372-83.