Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 141 (2018) 24–31

Procedia Computer Science

www.elsevier.com/locate/procedia

The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018)

A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing

Farouq Aliyu[a], Tarek Sheltami[a,*], Elhadi M. Shakshuki[b]

[a]*Computer Engineering Department King Fahd University of Petroleum and Minerals, Dammam, Saudi Arabia 31261*
[b]*Jodrey School of Computer Science, Acadia University, Wolfville, NS Canada B4P 2R6*

Abstract

Due to the large number of IoT devices available, data needed to be processed by cloud service providers has grown exponentially. This leads to increase in the latency of cloud services and by extension latency in many IoT applications. To reduce this latency, computing devices are installed at the edge of the network close to the user. These devices are called "Fog Nodes". They allow the user to process some data without going all the way to the data center. While the data centers are equipped with abundant resources (i.e. processors, energy and memory), the fog devices are not. This means traditional techniques for preventing intrusion are not applicable at the fog level, because they will incur more latency and/or energy consumption. Therefore, there is a need for low resource demanding, yet strong security system that will protect the fog layer from being attacked. This paper proposes an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) for Man in the Middle (MitM) attack at the fog layer. The IDS consists of IDS nodes that periodically interrogate nodes one hop away. The IPS uses lightweight encryption to prevent Man in the Middle attack and its variants (i.e. Eavesdropping, Packet Modification and Wormhole attack).

Keywords: Fog Computing; Man in the Middle Attack; Intrusion Detection System; Intrusion Prevention System; Network Security

1. Introduction

Volume, velocity and veracity of data has been increasing exponentially. By 2020, data in the Internet is foretold to reach 35 trillion gigabytes [1]. However, forty percent (40%) of these data needs to be analyzed on devices physically close to the Internet of Things [2]. Therefore, it is necessary to bring computing devices physically close to the edge of the cloud, closer to IoT devices. This led to the development of Fog computing.

Fog– or Edge computing is a form of computing where (Fog) devices physically close to end user devices (Things) process data on behalf of the cloud in order to reduce latency. Any device with computing, storage and network connectivity can be deemed a fog node/device [3]. Fog and cloud complement each other. They provide interdependent

* Corresponding author. Tel.: +966-13-860-4678 ; fax: +966-13-860-3059.
E-mail address: tarek@kfupm.edu.sa

1877-0509
10.1016/j.procs.2018.10.125

and mutually beneficial services in order to make communication, computing, control and storage possible throughout the system. Therefore, attacking the fog node is as good as attacking the cloud, save it is easier since it has more limited resources. One of the most notorious attacks in computer networks is Man in the Middle (MitM) attack [4, 5]

MitM attack is a type of attack carried out by a malicious internal user on two computers by pretending to one that he is the other [6]. MitM can be of two categories [7]: Eavesdropping and Manipulation. Eavesdropping is passive as the adversary is only interested in the information passing through. In Manipulation MitM, the adversary changes data while masquerading it as the original sender.

Moreover, motivation to detect and prevent MitM is high, because it is arguably the most common attack in Fog computing systems [8, 9].This is due to the fact that fog architecture is inherently similar to a MitM attack, since fog node is in-between the cloud and the end device (Thing). Thus, enabling an attacker to hide in plain sight. Also, fog nodes process deeply personal information such as medical history, medication and persons state of health. They also process other crucial information such as speed, direction and destination of vehicles. In any case, such information may prove disastrous in the wrong hands. Furthermore, fog nodes are more attractive to attackers because they have less computing power and are closer to the attacker than to the cloud [10].

However, due to large number and variety of nodes in fog computing, conventional security techniques such as security credential may be difficult if not impossible to apply [11]. Moreover, fog nodes are often resource constrained; therefore, energy efficient security techniques are necessary. The aim of this research is to determine cost effective techniques for detecting and preventing MitM attack, at the fog level in a fog computing network. The proposed system uses Intrusion Detection System (IDS) nodes strategically placed in the network in order to achieve attack detection, and it uses lightweight encryption to prevent attack.

The remaining part of this paper is as follows: Section 2 provides a literature review of Intrusion Detection Systems (IPS) and Intrusion Detection Systems (IDS) currently available. Due to lack of research in IPS and/or IDS system in fog computing, IoT systems and Wireless Sensor Networks (WSN) are discussed because of their uncanny resemblance to fog system. Section 3 describes the proposed system and its network model. Finally, Section 4 discusses the performance of the proposed system. Section 5 provides the conclusions and future work.

2. Literature Review

Several works have been carried out in securing IoT from Man in the Middle (MitM) attack [12, 13, 14]. The most common solution to MitM attacks is to encrypt communication with either symmetric or asymmetric algorithms, mutual authentication, and ensuring that compromised nodes have been isolated [10]. However, the aforementioned solution has not been tailored for fog computing – there are no standard security measures and certifications tailored to Fog computing [5, 10].

Authors in [15] designed authentication system for the IoT. The system can prevent attacks like eavesdropping, MitM, key control, and replay attacks. The system moves computation to a device with more computing resources known as the Registration Authority (RA), who is responsible for authenticating as well as cataloging Things in the network. In the case of fog computing, the fog node will be in the perfect position to handle this job. However, if the fog node is compromised the whole network is compromised. In [8], the authors developed security system for cloud computing using public key cryptography and IoT authentication scheme. Nonetheless, traditional PKI based authentication is not suited to Fog computing due to huge computation and communication overhead [16]. Therefore, techniques are needed to mask these overheads.

Detecting MitM attack solely hinges on observing the behavior of nodes in the network. Mohanapriya *et. al.* [17], developed a detection technique for Dynamic Source Routing Protocol (DSR) from gray hole attack. Gray hole attack is an attack where nodes selectively destroy some packets they receive while forwarding others. The authors developed a non-cryptographic technique where the destination node detects the presence of gray hole attackers in the route based on the difference in number of data packets sent by the source node and those actually received by the destination node. IDS nodes are notified of suspected nodes. The IDS broadcasts the information of the malicious nodes to other nodes in the network thereby isolating them. MitM attacks do not destroy packets. As such, they cannot be detected by the number of packets missed; since a packet is eventually received by the destination node. Aziz *et al.* [18], proposed a MitM detection system that uses arrival time of packets to infer the possibility of MitM. When the difference between the expected arrival time of the packet and the actual arrival time of the packet exceeds a

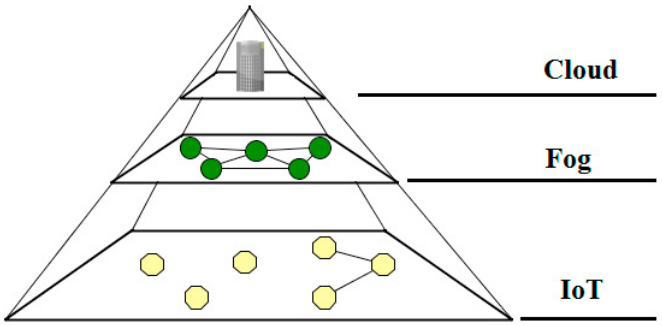


Fig. 1: Network architecture of a distributed fog network.

threshold T_{diff}, then an MitM attack is expected along the path. This technique may be difficult to apply in a noisy and/or heterogeneous environment, since arrival of packet may vary greatly due to the nature of the channel or the transmitting node.

The authors in [19], proposed a MAC-layer intrusion detection mechanism for detecting both MitM and Wormhole attack. Wormhole attack is a variant of MitM attack in which the adversary connects two distant part of the network [20]. In this technique [19], the sender and receiver secretly agreed on number of frames that will be transmitted without acknowledgement. Hence, an intruder is detected when it sends acknowledgement after receiving these packets. The authors were able to show that the system provides accurate detection at the expense of reduction in networks bandwidth.

Truelink [21], can be deemed a true IPS-IDS system against wormhole attack. The system uses Rendezvous phase and Authentication phases for IDS and IPS respectively. The rendezvous phase between two nodes i and j begins by the duo exchanging nonces α_i and β_j whose arrival time can be used as evidence of adjacency. The strict time constrain needed in this phase makes it difficult for an intruder to masquerade itself as a non-malicious node. In the Authentication phase, each of the nodes i and j exchange signed message (α_i, β_j): thus, mutually authenticating themselves as the original source of the aforementioned nonces.

To sum up what we learned in the literature, behaviors to look for in MitM attack are: 1) Change in content of packets sent. 2) Delay in arrival time of sent packets. 3) Change in the direction/destination of the packets. In this paper, an IPS-IDS system is proposed where special nodes known as IDS nodes are placed to interrogate fog nodes in the network and observe their behaviors based on the three aforementioned characteristics in order to conclude whether they are malicious nodes.

3. Proposed System

Figure 1 shows a typical distributed fog network. In this network, the IoT devices request for services from the fog nodes. The fog nodes usually have higher resources than the IoT devices and they are physically closer to the IoT devices compared to the cloud servers. Therefore, receiving services from the fog nodes reduces latency. The fog nodes and the IoT devices may use any medium and protocol to communicate. If the two use the same medium and protocol, both IoT and fog nodes enjoy the following: 1) Lower design complexity since only one network stack and the need for conversion of packets from one form to another is eliminated. 2) The absence of packet conversion, reduces energy consumption and latency of the network.

3.1. Network Model

Figure 2 shows the proposed system. The symmetry and proximity (one hop distance) to the fog nodes ensured in the deployment of the IDS nodes allows reduced latency. Each IDS is placed such that it is one hop away from the nodes it observes in a wheel spoke fashion. Whenever IDS node finds a compromised node or an intruder, it simply informs nodes close to it to cut off connection with the node.

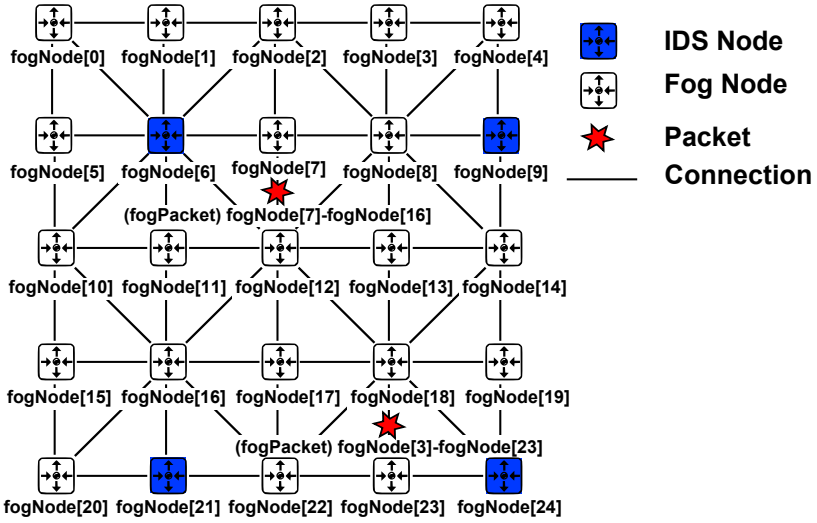


Fig. 2: The proposed fog network simulated using OMNET++.

In addition, packets are routed from source to destination by first moving the packets in a multi-hop fashion along the Y-axis (i.e. up or down). The packets move in this direction until they reach their destination's row. Then the packets move along the X-axis (i.e. backward or forward) until they reach their destination.

3.2. Attacker Model

In this research, it is assumed that the attacker carries out MitM in the fog layer. This allows him to intercept packets from the cloud, IoT and the fog layer. The attacker has equal or even more resources than the fog nodes but less resources than the cloud. Although the attacker may know about the existence of IDS nodes and the protocol they are using, he does not know the nature of the interrogation since it was chosen and pre-programmed before deployment of the nodes.

3.3. IPS-IDS System

The proposed system consists of two types of nodes; Fog Nodes (FN) and IDS Nodes. The FN provide services to the lower layer IoT devices at a reduced latency. On the deployment of the proposed system, IDS nodes acquire key from the cloud and distributes it to the FNs. All packets are encrypted (excluding header) in order to prevent intrusion. The proposed system uses Advanced Encryption System (AES) symmetric encryption technique, while encryption key is exchanged using Diffie-Hellman key exchange [22].

In addition, the IDS nodes periodically interrogates the FNs by sending interrogation packets. The interrogation packets are encrypted and (in this case) they consist of an integer value. The IDS node then observes the behaviour of the receiver: It expects the receiver to decrypt the packet and multiply the payload by 2, then encrypt the result and return it to the IDS. Multiplication by 2 is chosen because it consumes less time to carry out since it only involves shifting the integer to the left once. However, other more secured computation techniques like modulo operation may be used. When the returned packet fails this criteria, then the IDS can conclude that the node is malicious.

Furthermore, the IDS records the round trip time of the interrogation packet, when it exceeds certain threshold value then the node is an intruder that either copies or modifies the packets. However, if the packet is never replied, then we know that the node has received the packet and has send it elsewhere perhaps due to ignorance of the network protocol or the attacker is applying wormhole attack. Algorithm 1 and Table 1 are pseudocode and Truth table that show how the IDS node interrogates each node in order to fish out the compromised nodes respectively.

```
1: t_out ← timeout                                   // t_out and t_0 To be set by network administrator
2: t_0 ← allowed Delay                               // "i" are set of nodes under supervision of a given IDS node
3: for each fog node i do
4:    t_1 ← time()                                   // get current time
5:    t_2 ← 0
6:    pkt ← x                                        // x is randomly generated unsigned integer
7:    IDS sends pkt to fog node i
8:    repeat
9:       t_2 ← time()                                // While waiting for packet keep checking time
10:      Δ ← t_2 − t_1
11:   until (Reply_pkt received OR Δ > t_out )
12:   if ( Δ > t_out) then
13:      if (Reply_pkt not received) then
14:         attack is possibly wormhole              // Once Δ > t_out IDS stops listening for Reply_pkt
15:      end if
16:   else
17:      y ← Extract fog Node's answer from Reply_pkt   // Fog node should change x to 2x and reply to IDS
18:      if (Δ > t_0 AND Reply_pkt is received AND y ≠ x × 2) then
19:         attack is possibly packet altering or lack of context
20:      else if (Δ > t_0 AND Reply_pkt is received AND y = x × 2) then
21:         attack is possibly altering
22:      else if (Δ < t_0 AND Reply_pkt is received AND y ≠ x × 2) then
23:         attack is possibly eavesdropping
24:      else
25:         fog node is not compromised
26:      end if
27:   end if
28: end for
```

Algorithm 1: IDS investigation

Table 1: Truth table for the IDS

$\Delta > t_{out}$	$\Delta > t_0$	Reply_pkt received	$y \neq x \times 2$	Attack	Comment
0	0	0	0	0	Waiting for Reply_pkt
0	0	0	1	x	Not Possible, Reply_pkt is not yet received
0	0	1	0	0	Node is safe
0	0	1	1	1	Attack, eavesdropping or lack of context
0	1	0	0	x	Waiting for Reply_pkt
0	1	0	1	x	Not Possible, Reply_pkt is not yet received
0	1	1	0	1	Attack, possibly content altering
0	1	1	1	1	Attack, possibly altering content or lack of context
1	0	0	0	x	Not Possible, $t_{out} > t_0$
1	0	0	1	x	Not Possible, $t_{out} > t_0$
1	0	1	0	x	Not Possible, $t_{out} > t_0$
1	0	1	1	x	Not Possible, $t_{out} > t_0$
1	1	0	0	1	Attack, possibly wormhole attack
1	1	0	1	x	Not Possible, Reply_pkt is not received
1	1	1	0	x	Not Possible, if $\Delta > t_{out}$ Reply_pkt is ignored
1	1	1	1	x	Not Possible, if $\Delta > t_{out}$ Reply_pkt is ignored

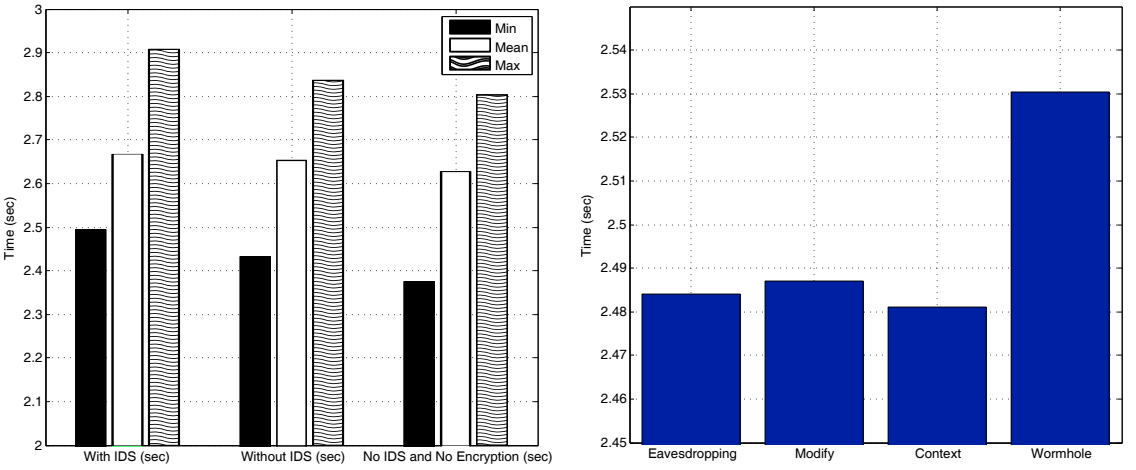
Table 2: Parameter Settings for Simulation

SN	Parameter	Value	Comment
1	Packet Size	1500 *byte*	Packet size in bytes
2	Process Delay (ρ_p)	0.5 *sec*	Time needed to process the data (seconds)
3	Investigate Time ($t_{investigate}$)	2 *sec*	Time IDS takes until the next investigation cycle
4	Packet Time-out	0.5 *sec*	Number of seconds to consider packet as lost
5	Volatge (V)	3.0 V	Voltage powering the system
6	idle (I_i)	320 μA	Wireless Hart idle listening current requirement
7	Transmission power (I_{tx})	19.3 mA	Wireless Hart transmission power
8	Reception power (I_{rx})	21.5 mA	Wireless Hart reception power
9	MCU Clock (f)	4.0 MHz	MCU processor is in MHz
10	Encryption/Decryption Cycle (N_{crypto})	7,429 *cycles*	Using AES, the clock cycles needed for encryption and decryption are 6,637 *cycles* and 7,429 *cycles* respectively. Max was chosen for worst case scenario
11	MCU Current (I_{run})	140 $\mu A/MHz$	Current needed while MCU processes data
12	MCU Sleep Current (I_{sleep})	37 $\mu A/MHz$	Current needed while MCU sleeps

4. Results

The proposed system is simulated using OMNET++. Table 2 enlists the simulation parameters used in the simulation. The energy and communication parameters are Wireless Hart parameters obtained from [23]. Wireless Hart is chosen because it is widely used in industrial application due to its robustness [24]. Also, AES is chosen as an IPS for the proposed system because it is considered lightweight and strong encryption technique [25]. The parameters are applied according to [25]. Furthermore, the simulation is run for four hundred seconds without any security mechanism, then it is executed with encryption and finally it is executed with both encryption and IDS node deployed.

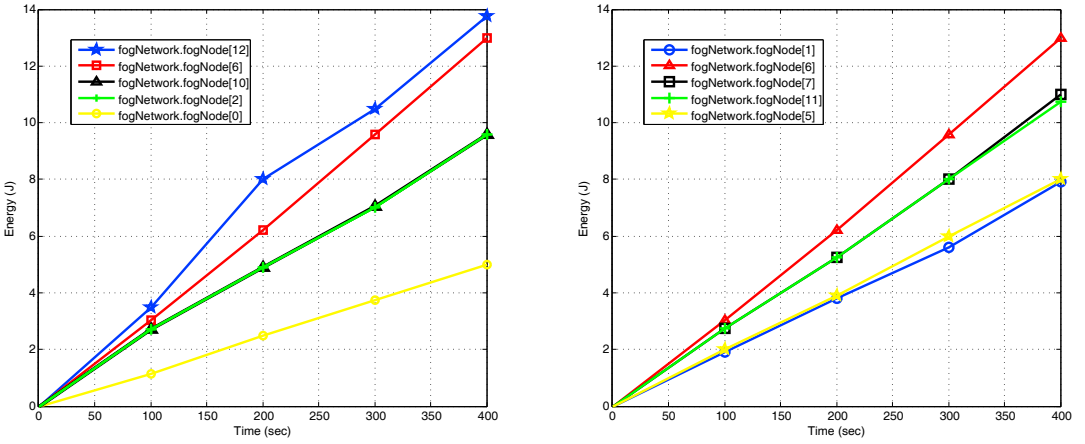
Figure 3(a) shows the latency of the system with IDS nodes and encryption, without IDS and without IDS and encryption. The average latency of the system with IDS is 2.6655 sec and the average latency of the system without IDS and encryption is 2.6268 sec this means the latency overhead for deploying IDS and IPS is 40 ms. Also, Figure 3(b) shows the amount of time taken before the IDS nodes detect an attack. Bearing in mind that the IDS node probe



(a) Latency of Services in the Fog Layer.

(b) Duration fognode[6] detects an attack.

Fig. 3: Latency of services and attack detection.



(a) Energy of Nodes 0, 2, 10, 12, and 6.

(b) Energy of Nodes 1, 7, 11, 5 and 6.

Fig. 4: Cumulative energy consumption of some selected node in the proposed system.

the nodes every $t_{investigate} = 2.0sec$ after the last investigation session (see: Table 2, SN 3), it can be seen that the time taken before an attack is discovered vary from $2.4810sec$ to $2.5303sec$. The time to detect Wormhole attack is longer because the IDS nodes have to ensure that the reply for IDS packet were not delayed due to noisy environment. The figure also shows that the IDS node takes $\approx 2.5sec$ to detect Wormhole attack. Since the IDS node waits for only $t_{investigate} = 2.0sec$ between investigations, then the actual discovery time, which is the time it takes the IDS node to detect an attack from the beginning of an investigation session is $t_{descovery} \approx 0.5sec$.

Figures 4(a) and 4(b) show the cumulative energy consumption of the system during the $400sec$ of simulation. The nodes 0, 1, 2, 5, 6, 7, 10, 11, and 12 were selected from the network in Figure 2. It can be seen that the energy of IDS in both cases is greater than the energy of the FNs. This is due to the fact that the IDS nodes periodically investigate each node one hope away. Hence, it has to communicate eight times while each FN has to communicate once during the investigation. In addition, the FN make less than eight transmissions between investigation sessions. This means in a busy network the IDS will consume less energy than the FNs, since the FNs will communicate among themselves more often than they communicate with the IDS nodes. Finally, the energy overhead incurred on the FNs by the IDS nodes is negligible since it only communicate once every investigation cycle.

5. Conclusion

In this research, the possibility of applying Intrusion Detection system (IDS) and Intrusion Prevention System (IPS) for Man in the Middle (MitM) attack using IDS nodes is investigated. An AES (128 bit, key and block size) encryption/decryption is used for IPS. In order to ensure reduced latency, special nodes known as IDS nodes were introduced to the system. Each IDS node interrogates fog nodes one-hop away and analyze their response in term of content, context and arrival time.

Latency overhead of as low as $40ms$ was observed when the proposed IDS-IPS system is deployed. However, this is at the expense of the investigation time which is inversely proportional to the networks latency and energy overhead of the network (IDS nodes inclusive). Therefore, fine tuning IDS investigation time is very important in ensuring the fog layer has low latency and it is energy efficient.

In the future we plan to change the allow delay (t_0) from a static value to a dynamic one. This will account for the non-deterministic latency of some communication media such as wireless. Thereby allowing the system to accurately detect wormhole, eavesdropping and packet altering attacks.

Acknowledgement

We are thankful to King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia for providing the necessary lab equipment and setup for experimentation. We would also like to thank Acadia University and Natural Sciences and Engineering Research Council (NSERC) of Canada for funding this research.

References

[1] G. Reinsel, J. Gantz, The digital universe decade-are you ready?, IDC White Paper.
[2] V. Turner, C. MacGillivray, J. Gaw, R. Clarke, M. Morales, B. Kraus, Idc futurescape: Worldwide internet of things 2015 predictions, in: IDC, 2014.
[3] F. Computing, the internet of things: Extend the cloud to where the things are (2016).
[4] C. Li, Z. Qin, E. Novak, Q. Li, Securing sdn infrastructure of iot–fog networks from mitm attacks, IEEE Internet of Things Journal 4 (5) (2017) 1156–1164. doi:10.1109/JIOT.2017.2685596.
[5] J. Ni, K. Zhang, X. Lin, X. S. Shen, Securing fog computing for internet of things applications: Challenges and solutions, IEEE Communications Surveys Tutorials 20 (1) (2018) 601–628. doi:10.1109/COMST.2017.2762345.
[6] Y. Desmedt, Man-in-the-middle attack, in: Encyclopedia of cryptography and security, Springer, 2011, pp. 759–759.
[7] B. Potter, B. Fleck, 802.11 Security, O'Reilly Series, O'Reilly Media, Incorporated, 2002.
URL https://books.google.com.sa/books?id=RVQ4GgKeEtgC
[8] I. Stojmenovic, S. Wen, The fog computing paradigm: Scenarios and security issues, in: 2014 Federated Conference on Computer Science and Information Systems, 2014, pp. 1–8. doi:10.15439/2014F503.
[9] B. N. B. Ekanayake, M. N. Halgamuge, A. Syed, Review: Security and Privacy Issues of Fog Computing for the Internet of Things (IoT), Springer International Publishing, Cham, 2018, pp. 139–174.
URL https://doi.org/10.1007/978-3-319-70688-7_7
[10] S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions, Journal of Cloud Computing 6 (1) (2017) 19.
[11] M. Chiang, T. Zhang, Fog and iot: An overview of research opportunities, IEEE Internet of Things Journal 3 (6) (2016) 854–864.
[12] K. Zhao, L. Ge, A survey on the internet of things security, in: Computational Intelligence and Security (CIS), 2013 9th International Conference on, IEEE, 2013, pp. 663–667.
[13] J.-c. YANG, B.-x. FANG, Security model and key technologies for the internet of things, The Journal of China Universities of Posts and Telecommunications 18 (2011) 109–112.
[14] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, IEEE, 2011, pp. 1–5.
[15] J. Liu, Y. Xiao, C. P. Chen, Authentication and access control in the internet of things, in: Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, IEEE, 2012, pp. 588–592.
[16] D. Kim, S. An, Efficient and scalable public key infrastructure for wireless sensor networks, in: The 2014 International Symposium on Networks, Computers and Communications, 2014, pp. 1–5. doi:10.1109/SNCC.2014.6866514.
[17] M. Mohanapriya, I. Krishnamurthi, Modified dsr protocol for detection and removal of selective black hole attack in manet, Computers & Electrical Engineering 40 (2) (2014) 530–538.
[18] B. Aziz, G. Hamilton, Detecting man-in-the-middle attacks by precise timing, in: 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 81–86. doi:10.1109/SECURWARE.2009.20.
[19] S. M. Glass, V. Muthukkumarasamy, M. Portmann, Detecting man-in-the-middle and wormhole attacks in wireless mesh networks, in: 2009 International Conference on Advanced Information Networking and Applications, 2009, pp. 530–538. doi:10.1109/AINA.2009.131.
[20] A. Pathan, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, CRC Press, 2016.
URL https://books.google.com.sa/books?id=ZtBnZoijaDcC
[21] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, Truelink: A practical countermeasure to the wormhole attack in wireless networks, in: Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference on, IEEE, 2006, pp. 75–84.
[22] D. P. Jablon, Strong password-only authenticated key exchange, ACM SIGCOMM Computer Communication Review 26 (5) (1996) 5–26.
[23] T. D. Chung, R. Ibrahim, V. S. Asirvadam, N. Saad, S. M. Hassan, Energy consumption analysis of wirelesshart adaptor for industrial wireless sensor actuator network, Procedia Computer Science 105 (2017) 227–234.
[24] M. Nixon, T. Round Rock, A comparison of wirelesshart and isa100. 11a, Whitepaper, Emerson Process Management (2012) 1–36.
[25] T. Eisenbarth, S. Kumar, A survey of lightweight-cryptography implementations, IEEE Design & Test of Computers 24 (6).