An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring

Fitwi, Alem, Chen, Yu, Zhou, Ning

Alem Fitwi, Yu Chen, Ning Zhou, "An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring," Proc. SPIE 11018, Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII, 110180L (7 May 2019); doi: 10.1117/12.2519006

SPIE.

Event: SPIE Defense + Commercial Sensing, 2019, Baltimore, Maryland, United States

An Agent-Administrator-based Security Mechanism for Distributed Sensors and Drones for Smart Grid Monitoring

Alem Fitwi[a], **Yu Chen***[a], **Ning Zhou**[a]
[a]Dept. of Electrical & Computer Engineering, Binghamton University, Binghamton, NY 13902

Abstract. Distributed sensors are the eyes and ears of a smart grid which provide information vital for monitoring and controlling the entire power generation, transmission, and distribution systems. Secure exchange of information among the sensing and decision-making entities is essential as failures may bring the entire system on its knees. With the rapid growth in the number of distributed sensors, drones have a myriad of applications. A swarm of drones could also be deployed in war zones and disaster-stricken areas where a secured intercommunication is of paramount importance for survivability and for successful mission completion. In this paper, a secure mechanism is proposed based on mobile agents to secure information exchange with minimum overhead. An Agent Administrator (AA) automatically clones and sends a secure mobile agent (SMA) to the target sensors or drones to scan and check their security status. Then, the dispatched SMAs send feedbacks to the server AA or other members. In case of sensors, the closest terminal unit to which the sensors are directly connected is designated as an AA, which is capable of checking authentication and scanning for vulnerabilities. In the case of drones, any one of them or multiple of them could be designated as the AA and the flagged feedback is broadcast to all other nodes or drones thereby providing them security status updates. A modified Nagle's Algorithm is also proposed to support real-time video transmission. The experimental results validate the effectiveness and convenience of the proposed system.

Keywords: Internet of Drones (IoD), Distributed Sensor Networks, Security, Authentication, Agent Administrator (AA), Secure Mobile Agent (SMA), Smart Grid.

*Corresponding Author: Yu Chen, ychen@binghamton.edu

1 INTRODUCTION

The rapid developments in mobile electronic equipment and systems have inspired the advent of drones, also known as unmanned aerial vehicles (UAVs). Among a wide spectrum of applications,[1–5] monitoring and connectivity relaying are two of the well-accepted roles for drones.[6,7] That is, the drones could be employed to play the role of relay towers when communication links happen to break due to natural disaster or deliberate vandalism. It is also important whenever monitoring and validation of data become necessary in an effort to fight source-spoofing and replay attacks. Without incorporating robust security mechanisms and services, however, drones cannot serve these purposes. Since 2007, along with the increase in their popularity, more and more attacks on drones have been reported, including video stealing, injection of malwares, and device hijacking.[8–10] Some commercially available WiFi based drones are vulnerable to basic security attacks.[11]

The attacks are usually put into three categories, namely confidentiality, integrity and availability attacks. The confidentiality attack refers to the loss or unauthorized access of information being exchanged between the drones and the command and control (C & C) center through illegitimate interception, to which many drones are vulnerable. It is often achieved using hacking, virus, malware, key loggers, Trojans, Hijacking, cross-layer attack, protocol-based attack, and identity spoofing. The integrity attack is often attributed to two threats, i.e., modification and fabrication. Modification refers to the tampering of current information whereas fabrication is the creation of

Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII, edited by
Ivan Kadar, Erik P. Blasch, Lynne L. Grewe, Proc. of SPIE Vol. 11018, 110180L

false information. Both demand the presence of integrity validation mechanism to be in place. The third category, availability attack, refers to interruption of communication or services usually caused by Denial of Service attack (DoS) and signal jamming.[8,12–18] Hence, efficient and robust security solutions are desperately needed to secure drone communications.

Mobile agents are self-controlled applications or mobile codes that can travel via a local area network or the Internet. They are capable of hopping from one node to another, performing predefined activities in each node, and interacting with other agents. They were originally designed and developed for a distributed computing paradigm.[19–24] Their mobility and ability to be deployed in a distributed environment can be exploited for continuous automated monitoring of the security of drones and smart grid sensors. It is feasible to customize the mobile agents to meet special requirements in drones and smart grid networks. They perform node authentication and authorization on top of continuous monitoring of the communicating nodes to prevent confidentiality, availability, and integrity attacks.

In this paper, a new Distributed, Agent-based Secure Mechanism for IoD and Smart grid sensors monitoring (DASMIS) scheme is proposed. It is designed to run over a hybrid of peer to peer (P2P) and client-server (C/S) network architecture with reduced protocol overheads for immediate and bandwidth-efficient communication. Each node is loaded with an initial status and equipped with a python-based agent, which is capable of scanning and detecting burned in ready-only node-IDs, Node IP Address, node MAC address, system calls made, installed applications, all running system programs and applications, and modifications. In addition, it performs data encryption and hashing, and reports changes to other peer nodes as well as to the server sitting in the C & C center. The agent securely authenticates nodes, enciphers the communication, and authorizes inter-node accesses. It prevents and detects attacks such as masquerading, modification, and DoS attacks.

The rest of this paper is organized as follows. Section 2 provides a brief discussion of previous works pertinent to this research. Then, the proposed DASMIS scheme is presented in Section 3 followed by Section 4 where the experimental setup is described and results are analyzed. Finally, the conclusive remarks and the direction of our ongoing research are presented in Section 5.

2 RELATED WORKS

2.1 Security in Smart Grid

Smart grid technologies are designed to leverage the benefits of the information and communication technologies (ICT) and incorporate them into electrical power networks for efficient generation, transmission, distribution, and billing of energy.[25] A smart grid is a digital network, which allows a duplex traffic flow between the utility and its customers equipped with smart sensing capability along the transmission and distribution lines, and various substations.[26,27] The smart grid technologies are proprietary and specifically designed to work with the electrical grid with the ability to digitally respond to the quickly and dynamically changing demand of electricity. As a cyber-physical system, it is more vulnerable to attacks that are able to exploit the inherent flaws in various layers, from the physical layer, communication layer, media access layer, to the networking layer.[28,29]

Eavesdropping, Jamming, and replay attacks are the typical attacks on the smart grid. An eavesdropping is a passive attack where the adversary listens to the network by means of wiretapping and analyzes the captured data without detectable interaction with the smart grid network.

Jamming is an active attack that disruptively interrupt the transmission of data. It occurs at the media access control (MAC) layer and the adversary can deliberately corrupt the control packets or exhaust the whole available channel causing DoS. The legitimate nodes will not be able to access the channel or medium. MAC and Address Resolution Protocol (ARP) flooding are DoS attacks directed on the medium access layer.[27–29]

While the security of ICT networks primarily focuses on information security, the smart grid security focuses on the safety of the plant or process. The security goals of smart grid are availability, integrity, and confidentiality. Availability is of the highest priority and confidentiality is ranked the lowest.[27,29,30] Because of these differences, today's smart grid is still very much prone to attacks despite the presence of many security products and solutions for ICT networks on the market. A number of researches pertinent to smart grid security have been conducted, especially following the discovery of the most threatening Supervisory Control And Data Acquisition (SCADA) network attack on the Iranian Nuclear Facilities.[26] There still exists a gaping hole begging for bridging.

2.2 Application and Security of the Internet of Drones

IoDs have a range of applications in search and rescue, military, transportation, surveillance, and relaying communication.[1,3,5,11] They are, however, susceptible to basic availability, integrity, and confidentiality attacks. Drones have a number of exploitable security weakness and they are prone to such attacks as cache-poisoning and buffers overflow, which could cause DoS or the disconnection of drones from the controllers. Penetration experiments were carried out on drones like the Wireless Parrot Bebop UAVs which revealed such vulnerabilities.[1,5,8,11]

Researchers have been endeavoring to develop security aware frameworks and layered drone network architectures to create an atmosphere enabling for well coordinated and secure interaction of drones. Several security challenges to the IoDs were studied and analyzed, which led to the proposal of a cyber-security threat model. The model is helpful for both designers and users of the drone systems in clearly understanding the details of the possible threats in order to identify and implement some solutions. However, it is not a full-fledged solution for the current security problems. It is just an initial framework on which others can build solutions. In addition, the fact that most security measures enforced in many drones are kept secret makes it difficult to identify which threats are impacting a certain vendor's drone system.[8] Extra scanning and penetration tests are required to identify the UAVs' flaws.

Likewise, a theoretical model for the architectural requirements of the IoD system was developed. A study was made on the Internet, air traffic control, and cellular networks to integrate them into a new drone traffic management system.[1,3] However, the security issues were not addressed. An overview of drone-assisted wireless relay communication was also provided without any consideration of the possible security threats and attacks.[5]

In short, despite the convenience of IoD for various applications, they have a number of unresolved security issues that make them perilous to use.

2.3 Mobile Agents: Applications and Security Issues

Mobile agents are self-controlled mobile programs that can travel via a local area network or the Internet. They are capable of hopping from node to node, performing predefined activities, and in-

teracting with other agents. They were originally designed and developed for the distributed computing paradigm. They could be applied in information retrieval, mobile computing, e-commerce, and network management because they have the capability to make complex problems simpler. However, their mobility from one network to another and from one system to another has made them a target of many security attacks, which have prevented them from being rendered into a number of applications.[19–22]

In this paper, multi-function, secure, semi-mobile agents are proposed for the smart grid network security.

3 DASMIS: A DISTRIBUTED AGENT BASED SECURITY MODEL

In this paper, a new DASMIS scheme is proposed, which is a hybrid, collapsed network architecture. The agents are installed on the server and nodes, which are capable of performing many security functions. The server sitting in the control and command center always assumes a server role whereas the IoD could conveniently assume both client and server roles. The whole shebangs of the design details are elucidated in the subsections that ensue.

3.1 Proposed Interconnection Model

Figure 1 illustrates the proposed networking model, which enables the nodes, drones as well as the smart grid wireless sensors, to exchange essential information in both distributed and centralized ways. A server, three drones, and three wireless sensors are considered for demonstration purpose as indicated in Fig. 1. The topology consists of three layers in terms of information exchanging. The server at the top of the topology receives information pertaining to the status of the drones and the information they collected from the wireless sensors in the smart grid. The drones are the middle layer, which relay the information about the status of the smart grid garnered by the wireless sensors sitting at the bottom layer. The sensors collect all required information regarding the operation and security status of the smart grid by means of their field instruments (or eyes and ears) and feed it to the hovering drones.

Figure 2 illustrates a scenario in which some of the sensors of a wind turbine generator (WTG) in a wind farm are presented. There are energy meters, anemometer, wind vane, generator vibration sensor, high and low torque shaft speed sensors, yawing angle sensor, pitching angle sensor, temperature sensor, oil level sensors, and safety chain status sensor. These sensors are often connected to a Remote Terminal Unit (RTU) installed in the top or bottom cabinets, which is in turn capable of establishing its connection with the Master Terminal Unit (MTU) in the control room. The RTU is equipped with the ability to convert/encapsulate electrical protocols into network protocols and it has computing and networking capabilities.

The proposed DASMIS model is designed to handle the situation in times of exigency or disaster when communication links break. It is not meant for permanent relaying or interconnection. Adversaries often study and record the system dynamics of the plant and use it to foil operators sitting in the control room while attacking the plant. When agents in the control room or operators observe very striking similarities between present and past system/plant dynamics, they can deploy a drone or swarm of drones to collect actual sensor measures. During the deployment, the drones and edge sensors interact and exchange status updates in a secure manner. Then, the drones send updates to the server whenever there is new update in comparison to the initially consented states.

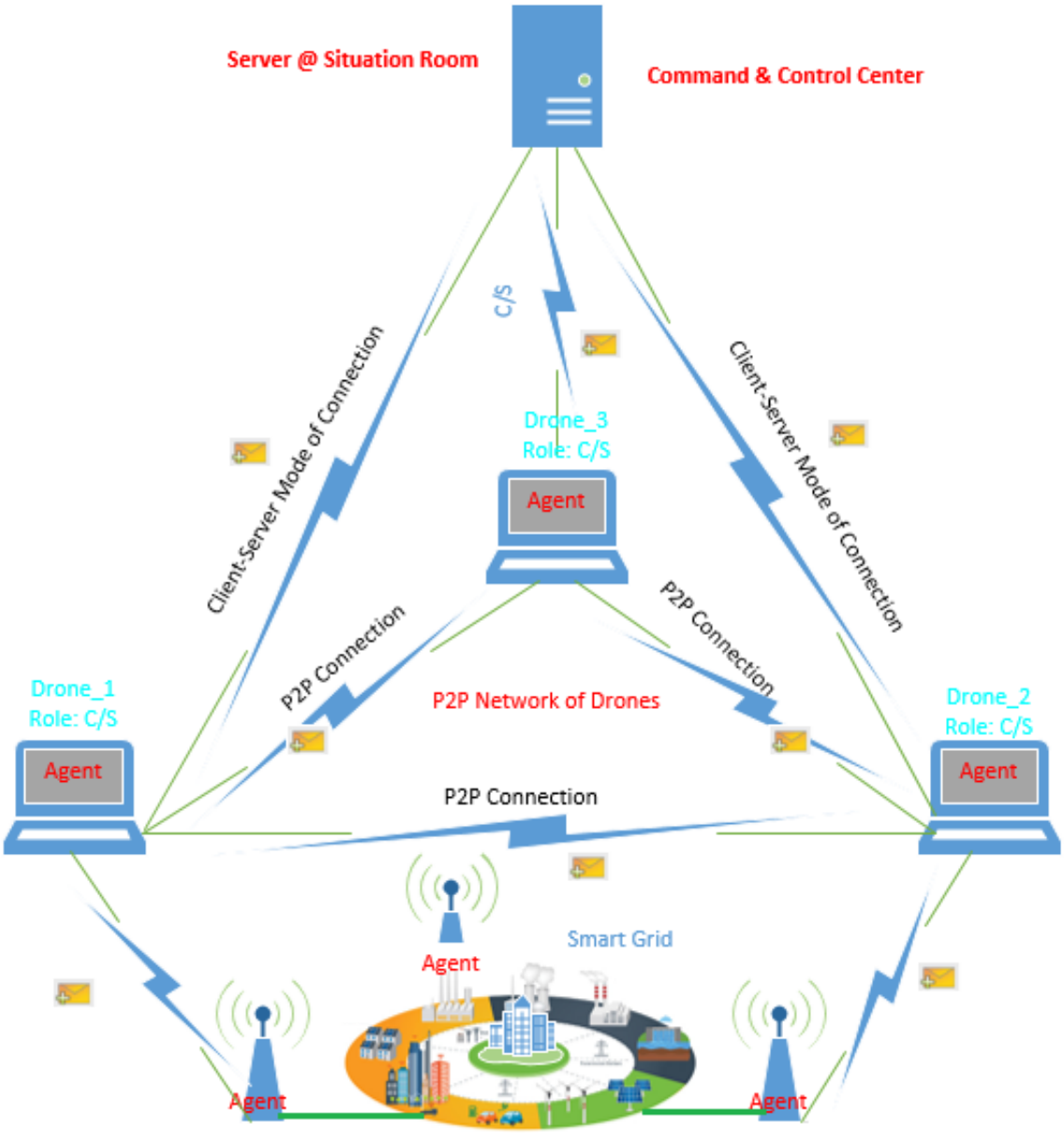

Fig 1 Proposed Interconnection Architecture.

The states are stored in every node as initial database (DB) of all nodes overall status where the details are elucidated in subsections 3.2 and 3.3. In terms of computing capabilities, the RTUs and the drones are considered as edge machines and the wireless standard considered is the IEEE 802.11ac.

To avoid the silly window syndrome or filling up of the channel with too many chunks of data, the Nagle's Algorithm[31] accumulates smaller-sized messages into a larger TCP packet before sending them across the communication channel. It waits until an acknowledgement is received for the sent packets. This is not friendly to delay-sensitive applications. In the DASMIS system, the Nagle's Algorithm is disabled when the IoDs are on a mission that requires real-time video an-

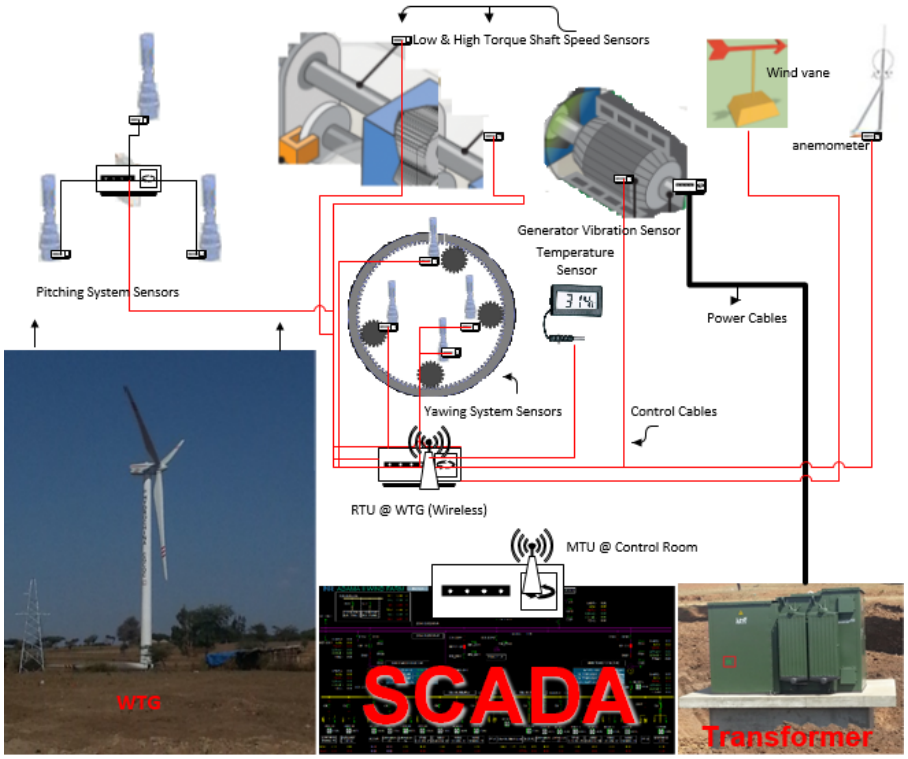

Fig 2 Some Smart Grid Sensors in a WTG Nacelle.

alytics. Besides, the Receive Window Auto-Tuning Level is normal and grows as to accommodate many scenarios. For instance, when an accident or natural disaster takes place in some part of the smart grid, the operator could deploy a swarm of drones to analyze the situation. The minimum size of a gray-scale image frame capable of conveying some meaningful information considered in our design analysis is about 100 KB (500x450 pixels). But the size of RGB images captured by modern digital cameras is in the order of MB or more because their resolution is 1024x768 pixels (1 Megapixel) or better. TV and movie recordings can be played back at a rate of 30 frames per second (fps) or 60fps. However, 60fps is a bit too smooth for humans to watch; as a result, almost all videos are recorded and played at a comfortable rate of 30fps. This has an implication on the budget for the allowable delay for real-time video analytics. That is, the total delay should be much smaller than one second for 30 frames or 30ms per frame.

Hence, the Nagle Algorithm can be disabled to allow real-time video analytic with no more ado contingent on minimum and maximum available data and receiver buffer sizes. Specifically, the algorithm is disabled if the size of the arriving data falls between the minimum data size (100 KB) and a maximum data size. The upper limit is set at 80% of the receiver buffer size so as to give the receiver enough time to inform the transmitter to slow down before being completely overwhelmed.

$$T_x = \frac{Data\_Size}{Available\_Bandwidth} \tag{1}$$

$$T_p = \frac{Distance\_Travelled}{Propagation\_Speed} \tag{2}$$

The lower and upper limits in the modified Nagle's Algorithm are set based on the time (T_x + T_p) the receiver needs to notify the transmitter just before it gets overwhelmed. The propagation delay and the transmission time are respectively computed based on Eq. (1) and Eq. (2) as to meet the budgeted delay. The AA acts like a light SDN in that it has some traffic engineering and management capabilities. The AA on the receiver side sends an alerting message to the sending end when the buffer is about 80% full. The sender then restores to nagling. One of the three reserved bits in the TCP header is used to apprise the sender to restore to nagling whenever about 80% of the buffer is full.

3.2 Agent Administrator

The AA is the heart of the security system of the DASMIS model. It is a program delegated by the server to continuously perform system scanning and to monitor any malicious activities in every node/drone in the mission and the wireless sensors installed in the smart grid of interest. The AA is deployed in each drone and the target smart grid sensors to enforce the required security policies and perform identity and security authentications. This version of the AA is said to be the client AA. The one installed on the server is capable of monitoring the status of all deployed client AA's.

As illustrated in Fig. 3, the server AA periodically sends a light-weight probing signal to the client-AA's, which then reply and inform the server that the AA's are alive and functioning well. If the AAs installed in the drones and sensors fail to respond due to some unexpected errors or failures, the server AA creates and dispatches another new AA by opening an Aglet platform and logging into the node as a root user using an automated shell script for Secure Shell (SSH). Hence, the client AA in our system is semi-mobile. It is initially installed on all nodes of interest with an initial DB of important node attributes, but if it fails or somehow gets corrupted, the server securely migrates a code and all required resources to create a new AA on the nodes on the mission.

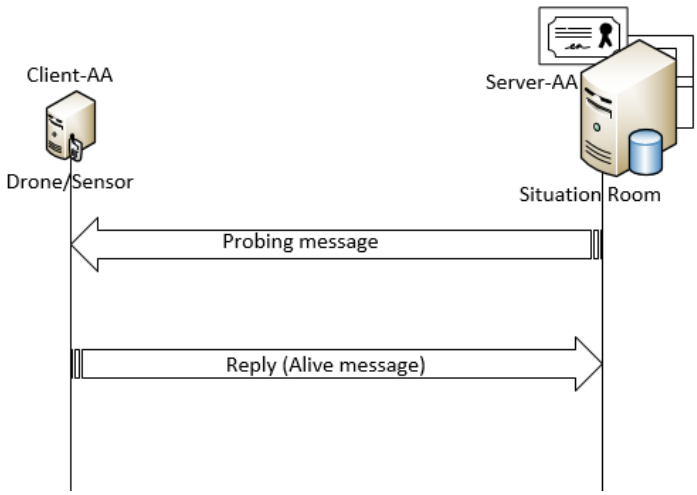

Fig 3 Client-Server AA's Control Message Exchange

The agent, developed based on python script, is a light-weight program that consumes less computing resources and bandwidth; but it is capable of performing a number of functions. The main ones are tersely explained as follows:

- ***Scanning and grabbing Node IDs***: The node IDs are the addresses used to identify the nodes or edge devices, including the MAC address, IP address, and a read-only address used to uniquely identify it. For security reasons, the ID is stored in a read-only memory (ROM) in that the AA can only read it but cannot change or delete it. The AA hashes the ID after accessing it whenever it wants to send a request or message to peer nodes or the server.

- ***Extracting System Program Attributes***: The AA is able to scan for the operating system (OS) running on the node and extract features, such as distribution type, Linux_distribution (applicable for Linux OS), system type (Windows/Linux/Mac/Android etc.), machine type, platform type, node name, processor type with details, version, updates or changes if any, dates of update, updated parts, and size change which are important in validating the integrity/authenticity of the node.

- ***Scanning for the Attributes of Application Programs*** : On top of the System Program, knowledge of the attributes of applications/programs installed in a device is very essential in studying vulnerabilities and possible security risks and in enforcing security countermeasures and patching the vulnerabilities of the device. The AA is designed to grab the attributes of each application including Product Name, Package Code, Transforms, Assignment Type, Package Name, Installed Product Name, Version String, Product ID, Product Icon, Install Location, Install Source, Install Date, URL Update Information, Update date and time, and Modification date and time.

- ***Capturing running Processes***: The AA creates a DB of the running processes along with their respective process IDs and keeps track of them. It also shares a copy of the DB to the server periodically. The server analyzes it in an effort to detect any anomalous activities or to identify resource hogging processes.

- ***Port Scanning***: Also known as fingerprinting, is a technique for determining which ports on a node are open. The AA performs the port scanning to garner information about which ports are open and listening (receiving information) on peer nodes. For instance, port 135 might be scanned and grabbed which is assigned for the Remote Procedure Call (RPC) service often used in client/server applications such as Exchange clients.

- ***TCP Packet Analysis and Traffic Engineering***: Here, the traffic engineering refers to improving the performance of the interconnecting network of our system via a dynamical analysis and regulation of data transmitted over the network. Depending on the size of the data being transmitted and the receiver TCP window-size, the AA not only can disable or enable the Nagle's algorithm but it can also manipulate the receiver's window settings.

- ***Hashing***: The AA can perform existing standard hashing functions. The selected default hashing algorithm is SHA224. Hashing is important for integrity checks and for the exchange of some messages vital for security checks in storage and bandwidth friendly manner.

- ***Encryption***: Security of the information exchanged between communicating parties is one of the top concerns. Advanced Encryption Standard (AES) is adopted in the DASMIS system.

- ***Identity and Security Authentication***: Identity authentication is conducted to block unauthorized accesses. A burned-in unique ID (stored in a ROM) of every node is initially hashed and shared to peers as part of the DB containing other features important for identity and security checks. When a node sends an access request to another peer node, it sends the hashes of its unique ID, MAC, and system. The AA on the receiving end uses this information for access control. The AA also contains a minimum access-control list and authorizes access to resources on the node accordingly.

- ***Reports CPU, Memory, VM, and Disk Performances***: The processor and the system memory are the most indispensable computing elements in a node that affect the overall system performance. Hence, tracking the performance of these vital elements of the drones is of paramount importance. The AA scans the performance and periodically shares a copy of it to the server situated in the C & C room. This early warning enables the operator to take action in time to counter potential DoS attacks. Figure 4 illustrates an example of a detailed performance report for the memory and the CPU of an edge device used in our experimental study.

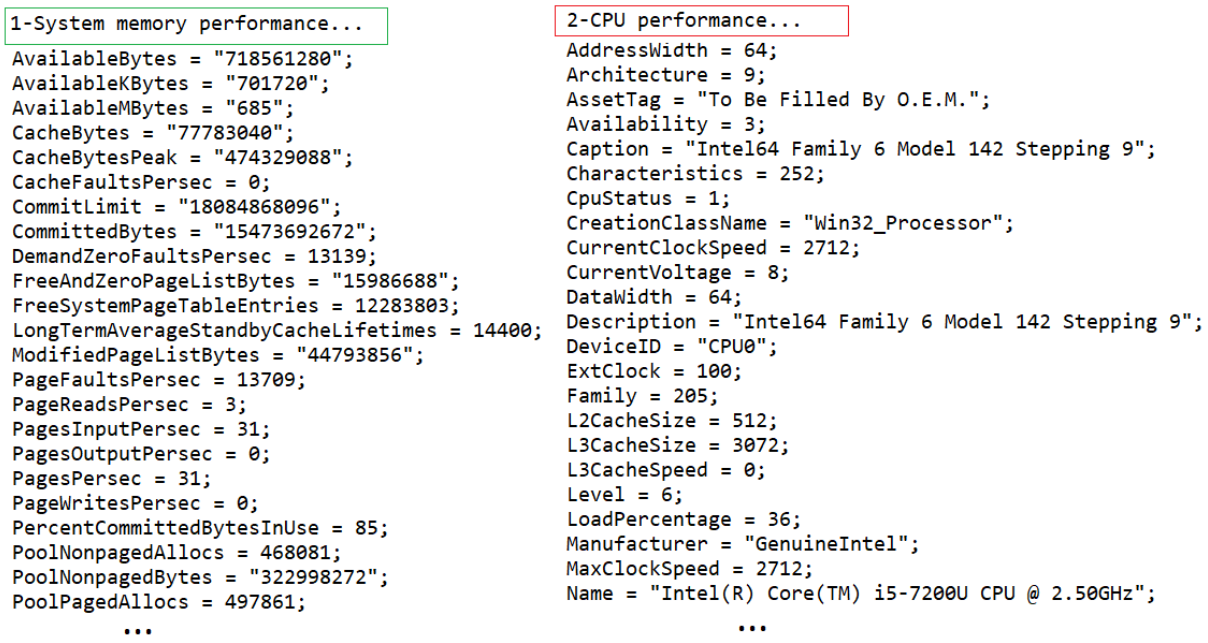

Fig 4 A partial detail of System Memory and CPU Performances of a Node Grabbed by the AA.

3.3 Security Countermeasures

The smart grid is vulnerable to tones of attacks. The most popular one is an availability attack coupled with a replay attack. Adversaries record the system dynamics for quite sometime and later replay it to deceive human operators or programs in the control room while covertly perpetrating something disruptive that would eventually cause service interruption. The sophisticated Stuxnet

attack is a well-known example that managed to destroy thousands of centrifuges in the Iranian nuclear facilities. The second but most devastating example is the cyberattack on Ukraine power grid in December 2015. It caused a temporary disruption of electricity supply to the consumers' premises from three energy distribution companies in Ukrain. The hackers managed to successfully compromise the information systems of these suppliers and switched off 30 substations leaving 230 thousand people without electricity for a duration of 1 to 6 hours.[32,33] This has sent shocking waves to the rest of the world as a result of which the efforts to reinforce the security of smart grids have gained a huge momentum.

The DASMIS system leverages drones and wireless sensors to detect and prevent attacks on the smart grid. The countermeasures are based on the analysis of the information collected through expansive scanning of edge device attributes. The major policies and the bandwidth aware countermeasures taken by the DASMIS system are itemized and explained as follows.

- ***Countermeasures against Availability Attacks***: Availability is one of the three main goals of any security mechanism. It ensures that information or services are accessible to authorized parties. Nowadays, plants like smart grids and information websites are often taken down by DoS or Distributed DoS (DDoS) attacks. Some of the commonest methods of attack that make information, resources or services unavailable to the legitimate users include physical damage or interruption, Ping Flood, Smurf Attack, SYN Attack, and Buffer Overflow. They deny the legitimate users access to the system, degrade the performance of the system, or disrupt the normal functionality of the system.

  In the DASMIS system, to prevent DoS and hijacking attacks on the covey of drones and wireless sensors, a security measure that enforces the analysis of requests to authenticate the identity of a source is implemented. All AA's have access to an encrypted DB stored in every edge device (drone or sensor), initially created by the server. It contains information about the unique node IDs, MAC addresses, system program attributes, and application program attributes. It is updated by the server whenever a legitimate update is committed. Hence, the AA on the receiving end extracts this information from the request and perform multiple comparisons to make identity and security authentication of the source as depicted in Fig. 5 and share any presumed security risks with peers and the server. Hence, intra-peer access or access to the server is restricted to the members in the mission in such a way. The AA's on the peers independently and in collaboration with the server can stop any unauthorized access or superfluous requests that could potentially result in DoS.

  What is more, the server periodically receives reports of the system performance, and a menu of the running processes. Then, it takes preventive measures after performing simple analysis to identify which processing is unfairly hogging the computing resources and bandwidth which could potentially cause a DoS attack.

- ***Countermeasures against Integrity Attacks***: Generally the integrity of information refers to preventing information from being modified by unauthorized parties. That is ensuring that the information is delivered to the authorized communicating party intact and it can be changed only by legitimate users. The underlying principle here is that information has value only if it is not tampered by illegitimate users. Hence, the integrity of the information sent

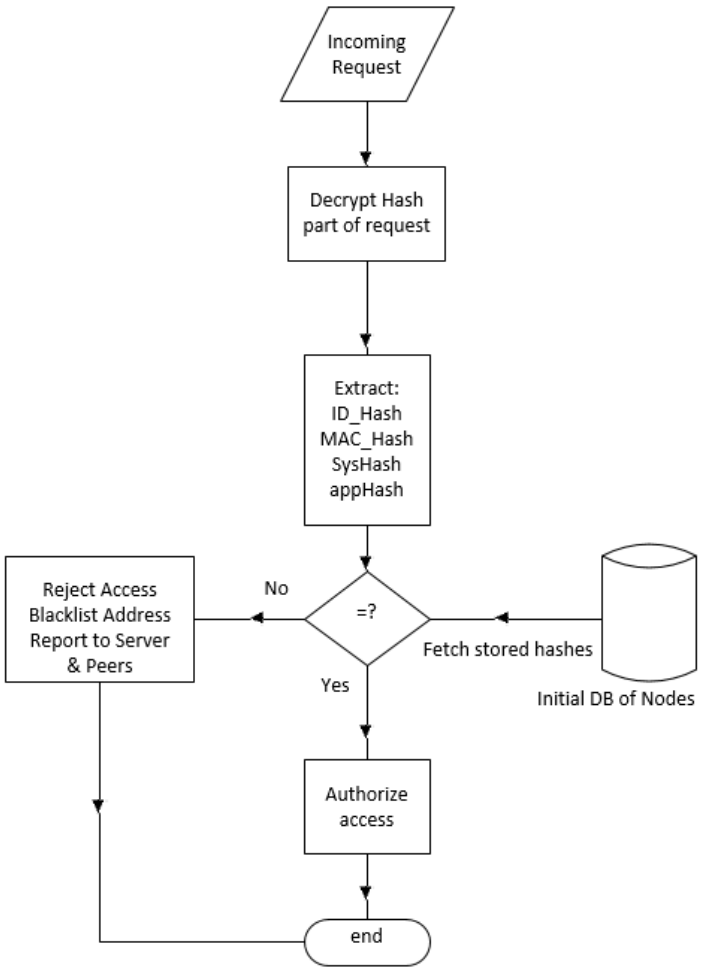

Fig 5 Simplified Request's Source Identity and Security Authentication

over a communication channel or stored is checked by comparing the hashes generated at the start of communication or time of storing and time of reception or use. The default hashing algorithm in our AA is SHA224; other hashing algorithms can be employed, though.

In our proposed system, the integrity thing also refers to edge device security. The integrity or authenticity of the drones or sensors is first checked before their requests are processed. The information they send could be considered legitimate to prevent source spoofing attacks. As portrayed in Fig. 5, the hashes of the unique ID of the requesting drone or sensor loaded on ROM, the MAC address, the attributes of the system programs, and the attributes of the applications are compared against an initial DB to verify the integrity/authenticity of the supplicant source.

The covey of drones could be deployed to areas where the smart grid infrastructures are installed or whenever something suspicious is detected to ensure that the operators in the control room are not beguiled by replay attacks.

- ***Countermeasures against Confidentiality Attacks***: Confidentiality refers to the privacy of

the information exchanged by communicating parties or the information stored in each node. And information is the most valued asset in the eyes of confidentiality measures. Hence, we need to have a mechanism to protect the information from any disclosure to unauthorized parties. The best-known solution for confidentiality problems is the use of cryptographic methods.

In the DASMIS, every communication is encrypted. The AA's are capable of performing encryption and decryption operations. The standard AES was experimented and works fine. We opted to stick to the AES because it has a proven security track record. No significant attack has been successfully perpetrated on it to date since its official declaration as the Federal Information Processing Standard (FIPS) in 2001. For the key exchange among communicating parties, the Diffie-Hellman protocol was adopted where the key exchange is achieved through the sharing of secret nuances between the AA's of the communicating parties in lieu of actual keys.

4 EXPERIMENTAL STUDY

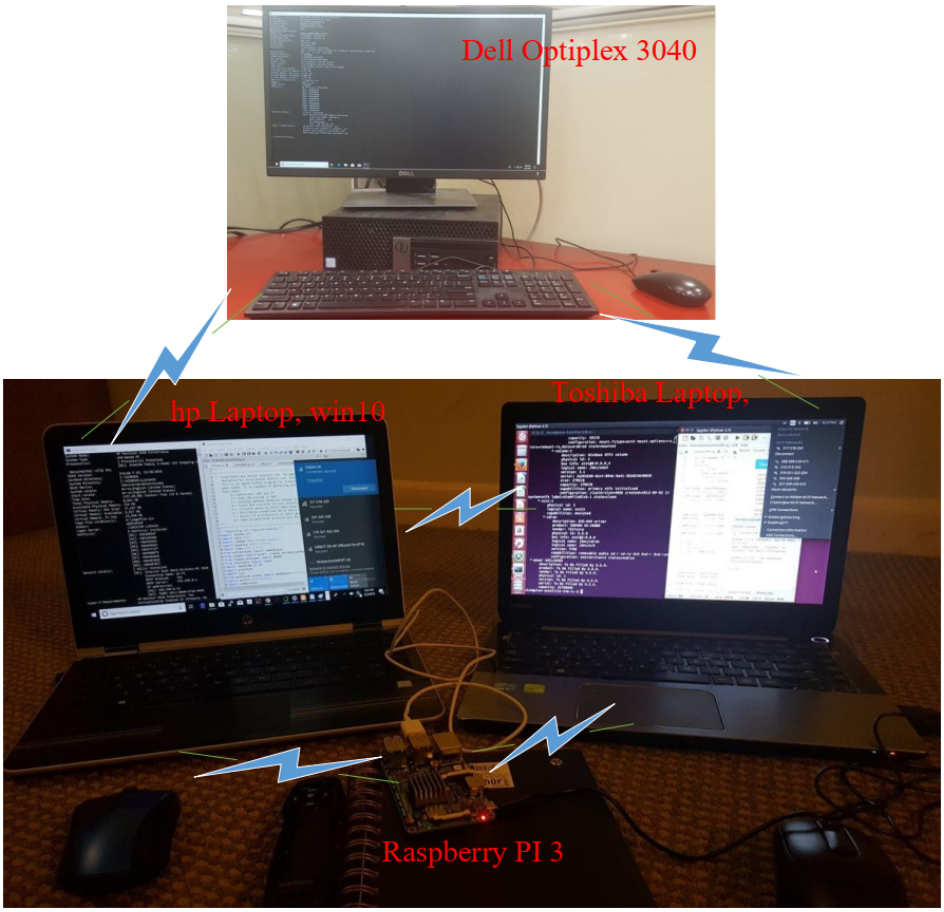

Fig 6 Experimental Setup with a Cloudlet server and Edge devices.

4.1 Experimental Setup

The proposed system shown in Fig. 1 was tested and validated experimentally with the following setup. A Windows server 2012 R2 virtual machine (VM) functions as the control room server, three Ubuntu 15.10 VMs as drones, a Windows 7 virtual machine as a wireless sensor, and a light Windows XP Virtual Machine as another wireless sensor. Then, following the successful tests in a virtual environment, a physical platform was created for an emulation study. A Dell Optiplex 3040 Desktop PC was used as a cloudlet server, whose configuration was: Operating system Windows 10, 3.192GHz CPU, and 4GB RAM. Two laptops were used to emulate the drones, one of which is an HP laptop that runs Windows 10 Operating system on Intel core i5 CPU and 4GB RAM, another is a Toshiba laptop with the Operating system of Ubuntu 14.04LTS, 1.8GHz CPU, and 4GB RAM. A Raspberry PI 3 worked as a wireless sensor. The system is portrayed in Fig. 6.

4.2 Result Analysis

Both the virtual and physical settings have produced results that corroborate the proposed DASMIS model. All possible scenarios were tested and all gave positive results. That is, the modified Nagle's Algorithm was tested and verified by sending a real-time video capture at one node with the help of a python script and openCV at 30 fps to two nodes with receiver window sizes of 65,535 B and 14,600 B.

Besides, all other functionality of the AA were tested and the results are very encouraging. For the demonstration purpose, two snapshots are presented. Figure 7 illustrates the identity and security authentication result of a node that sent a request to another node. As described in subsection 3.3, the part of the request containing hashed information is first decrypted, and then the ID_Hash, MAC_Hash, SysHash, and appHash are extracted and compared against a pre-configured DB stored in the receiving node. In this case, everything matched perfectly and the request was processed and authorized.

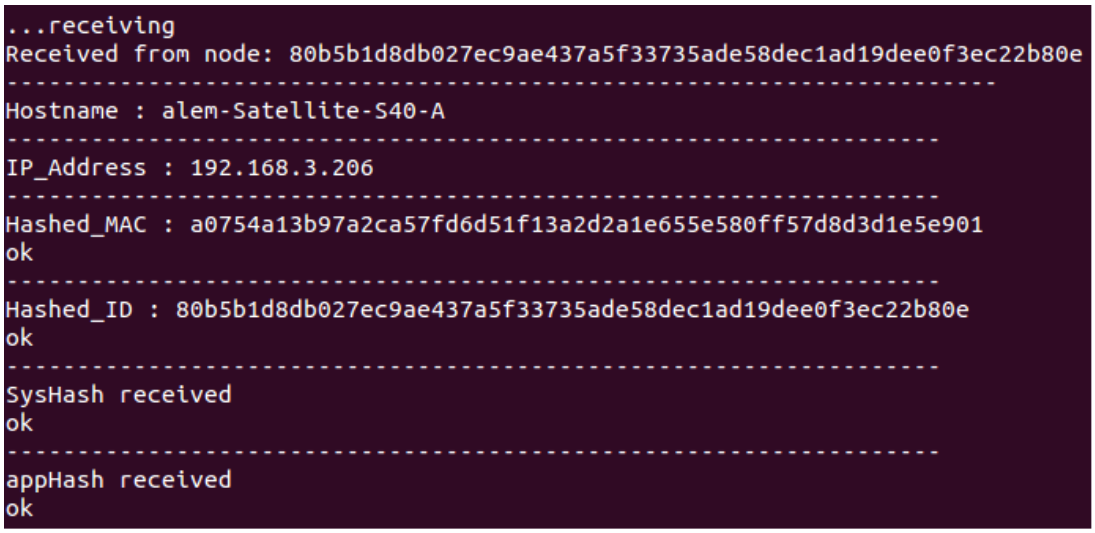

Fig 7 Results of Identity & Security Authentication on Request sent by a member Node

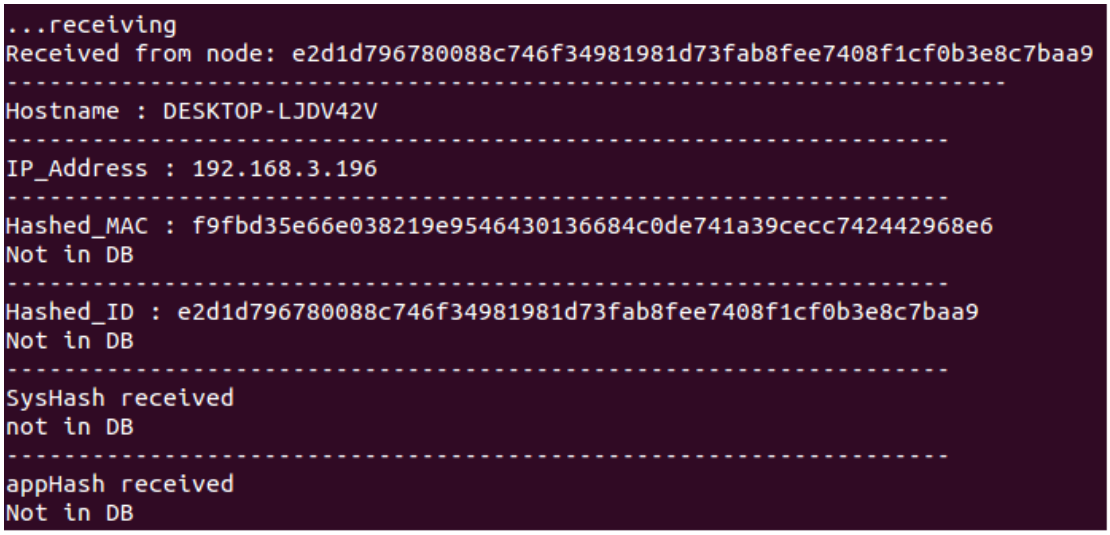

Fig 8 Results of Identity & Security Authentication on Request sent by a non-member Node

Figure 8 portrays a scenario where a request was rejected, blacklisted, and reported as an allegedly malicious node to peers in the group and the server. For testing purpose, the request was sent from a node which is not a member of the nodes in the mission. Then, after all preliminary processes like decrypting the incoming hashes and those in the local DB, a comparison was made. As expected, no match was found in all comparisons and then, the request was rejected, blacklisted, and reported.

Our proposed system is computing resources and bandwidth conscious due to the fact that all nuances of a node required for identity and security authentication and access authorization are exchanged in a compact or hashed form. It is convenient for edge device with limited computing capabilities. In addition, the results of the validating experiments show that our proposed model is efficient and applicable for IoDs deployed to a special mission like smart grid monitoring (the one considered in this work), coordinated attacks in battle zones, search and rescue, and collaborative IoD based smart surveillance.

5 CONCLUSIONS

Distributed sensors, as part of a smart grid, are the vital components of power generation, transmission, and distribution systems. Drones are the emerging and promising technologies capable of changing the way of information collection, monitoring and surveillance. However, both drones and the smart grid are prone to many attacks against availability, integrity, and privacy. Drones can be hijacked and weaponized or stolen. DoS attacks could be perpetrated on them, and the information they gather could be accessed by unauthorized users.

In this paper, we proposed a DASMIS system for a secure deployment of a covey of drones for a special mission, particularly smart grid monitoring when it is needed. A smart and light-weight AA was developed. It is capable of performing identity and security authentication at each node. Experimental results show that the proposed model could be conveniently applied for a swarm of drones on a special mission. It is a secure, and computing resource and bandwidth aware model.

The ultimate goal of this study is to build a full-fledged, secure, and computing resources and bandwidth-conscious framework for IoD-based smart surveillance. We will continue to investigate, and enrich it to a full-blown system over time.

References

1 Gharibi, M., Boutaba, R., and Waslander, S. L., "Internet of drones," *IEEE Access* **4**, 1148–1162 (2016).

2 Wang, J., Feng, Z., Chen, Z., George, S., Bala, M., Pillai, P., Yang, S.-W., and Satyanarayanan, M., "Bandwidth-efficient live video analytics for drones via edge computing," in [*2018 IEEE/ACM Symposium on Edge Computing (SEC)*], 159–173, IEEE (2018).

3 Kinge, R., Gawande, P., S. ingle, A., and Badhe, S., "Internet of drones," *nternational Journal of Research in Advent Technology (IJRAT) (E-ISSN: 2321-9637)* (2017).

4 Roder, A., Choo, K.-K. R., and Le-Khac, N.-A., "Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study," *arXiv preprint arXiv:1804.08649* (2018).

5 Zeng, Y., Zhang, R., and Lim, T. J., "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Communications Magazine* **54**(5), 36–42 (2016).

6 Chen, N., Chen, Y., Song, S., Huang, C.-T., and Ye, X., "Smart urban surveillance using fog computing," in [*2016 IEEE/ACM Symposium on Edge Computing (SEC)*], 95–96, IEEE (2016).

7 Chen, N. and Chen, Y., "Smart city surveillance at the network edge in the era of iot: opportunities and challenges," in [*Smart Cities*], 153–176, Springer (2018).

8 Javaid, A. Y., Sun, W., Devabhaktuni, V. K., and Alam, M., "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in [*2012 IEEE Conference on Technologies for Homeland Security (HST)*], 585–590, IEEE (2012).

9 Arthur, C., "Skygrabber: the $26 software used by insurgents to hack into us drones," *The Guardian* **17** (2009).

10 Summerville, D. H., Zach, K. M., and Chen, Y., "Ultra-lightweight deep packet anomaly detection for internet of things devices," in [*2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*], 1–8, IEEE (2015).

11 Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., Robinson, W. H., and Alexis, W., "Securing commercial wifi-based uavs from common security attacks," in [*MILCOM 2016-2016 IEEE Military Communications Conference*], 1213–1218, IEEE (2016).

12 Northcutt, S., "Are satellites vulnerable to hackers?," *SANS Technology Institute, May* **15** (2007).

13 Meunier, P., "Drone flaw known since 1990s," *Center for Education and Research in Information Assurance and Security, Purdue University* (2009).

14 Gouripeddi, V., "Improvement of security in uas communication and navigation using ads-b," (2016).

15 Bichler, S. F., "Mitigating cyber security risk in satellite ground systems," tech. rep., Air Command And Staff College Maxwell Air Force Base United States (2015).

16 Wang, W., Sun, Y., Li, H., and Han, Z., "Cross-layer attack and defense in cognitive radio networks," in [*2010 IEEE Global Telecommunications Conference GLOBECOM 2010*], 1–6, IEEE (2010).
17 Alves-Foss, J., "Multi-protocol attacks and the public key infrastructure," in [*Proc. 21st National Information Systems Security Conference*], 566–576 (1998).
18 Fitwi, A. H. and Nouh, S., "Performance analysis of chaotic encryption using a shared image as a key," *Zede Journal* **28**, 17–29 (2011).
19 Alami-Kamouri, S., Orhanou, G., and Elhajji, S., "Overview of mobile agents and security," in [*2016 International Conference on Engineering & MIS (ICEMIS)*], 1–5, IEEE (2016).
20 Mahmoodi, M. and Varnamkhasti, M. M., "A secure communication in mobile agent system," *arXiv preprint arXiv:1402.0886* (2014).
21 Dadhich, P., Dutta, K., and Govil, M., "Security issues in mobile agents," *International Journal of Computer Applications* **11**(4), 1–7 (2010).
22 Nouh, S. and Admassu, T., "Threats and trusted countermeasures using a security protocol in the agent space," *Zede Journal* **26**, 53–63 (2009).
23 Braun, P. and Rossak, W. R., [*Mobile agents: Basic concepts, mobility models, and the tracy toolkit*], Elsevier (2005).
24 Versteeg, S., "Languages for mobile agents," *arXiv preprint arXiv:1507.01656* (2015).
25 Yang, Z., Chen, N., Chen, Y., and Zhou, N., "A novel pmu fog based early anomaly detection for an efficient wide area pmu network," in [*2018 IEEE 2nd International Conference on Fog and Edge Computing (ICFEC)*], 1–10, IEEE (2018).
26 Sanjab, A., Saad, W., Guvenc, I., Sarwat, A., and Biswas, S., "Smart grid security: Threats, challenges, and solutions," *arXiv preprint arXiv:1606.06992* (2016).
27 Aloul, F., Al-Ali, A., Al-Dalky, R., Al-Mardini, M., and El-Hajj, W., "Smart grid security: Threats, vulnerabilities and solutions," *International Journal of Smart Grid and Clean Energy* **1**(1), 1–6 (2012).
28 Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., and Hubaux, J.-P., "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)* **45**(3), 25 (2013).
29 Mo, Y., Chabukswar, R., and Sinopoli, B., "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology* **22**(4), 1396–1407 (2014).
30 Otuoze, A. O., Mustafa, M. W., and Larik, R. M., "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology* **5**(3), 468–483 (2018).
31 Minshall, G., Saito, Y., Mogul, J. C., and Verghese, B., "Application performance pitfalls and tcp's nagle algorithm," *ACM SIGMETRICS Performance Evaluation Review* **27**(4), 36–44 (2000).
32 Zetter, K., "Inside the cunning, unprecedented hack of ukraines power grid, wired, 3 march 2016," (2017).
33 Whitehead, D. E., Owens, K., Gammel, D., and Smith, J., "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in [*2017 70th Annual Conference for Protective Relay Engineers (CPRE)*], 1–8, IEEE (2017).