Secure Routing for MANET Connected Internet of Things Systems

Jonny Karlsson
Department of Business Management and Analytics
Arcada University of Applied Sciences
Helsinki, Finland
e-mail: jonny.karlsson@arcada.fi

Laurence S. Dooley
School of Computing and Communications
The Open University
Milton Keynes, United Kingdom
e-mail: laurence.dooley@open.ac.uk

Göran Pulkkis
Department of Business Management and Analytics
Arcada University of Applied Sciences
Helsinki, Finland
e-mail: goran.pulkkis@arcada.fi

***Abstract*—This paper presents a contemporary review of communication architectures and topographies for MANET-connected Internet-of-Things (IoT) systems. Routing protocols for multi-hop MANETs are analyzed with a focus on the standardized Routing Protocol for Low-power and Lossy Networks. Various security threats and vulnerabilities in current MANET routing are described and security enhanced routing protocols and trust models presented as methodologies for supporting secure routing. Finally, the paper identifies some key research challenges in the emerging domain of MANET-IoT connectivity.**

Keywords-IoT; MANET; routing; network security; RPL; trusted device; sensor network

I. INTRODUCTION

Wireless sensor networks (WSN) and wireless sensor and actuator networks (WSAN) both play a key role in the implementation of Internet of Things (IoT) systems since they represent the interaction between today's computational systems and the physical world. In a WSAN, both sensors and actuators control the physical environment with quantities, such as temperature, pressure, sound level and light intensity being continuously measured by devices connected to either a WSN or a WSAN. Measured data are sent by wireless communications to processing devices for analysis and requisite control data transmitted back to WSAN connected actuators. Both WSNs and WSANs are used in a myriad of application domains including environmental monitoring and location/tracking, critical industrial applications, smart grids and healthcare. WSN and WSAN communications usually involve multi-hop which mandates routing functionality of all connected devices that are not end system nodes. They are also by their nature, low-power and lossy networks (LLN), being realized according to a particular networking standard like IEEE 802.15.4 [1], ZigBee [2], Bluetooth [3], WirelessHART [4], ISA-100.11a [5] or as mobile ad-hoc networks (MANET), which are multi-hop, self-configuring networks [6], [7].

This position paper presents some new insights into emerging issues relating to routing security for MANET-connected IoT systems. The aim is to critically evaluate the suitability of existing standards and other hitherto proposed routing security solutions along with the identification of current research challenges involved in designing secure routing protocols for MANET connected IoT systems.

The remainder of this paper is organised as follows: Section II explains all the possible routing paths used in the underlying communications architecture of MANET-connected IoT systems, before Section III reviews existing routing protocols available for this architecture. Section IV examines the threats and vulnerabilities to routing for which new security solutions are required, while Section V describes some existing methodologies for implementing secure routing in MANET-connected IoT systems. Section outlines current domain research challenges with Section VI presenting some concluding comments and identifying emerging trends.

II. COMMUNICATION ARCHITECTURES

The range of communication options requiring secure routing for MANET connected IoT devices are depicted in Table I. For example, an IoT device can be connected to a MANET node. It can also be a MANET node, and be either connected to an Internet node or be an actual Internet node. An IoT device connected to a MANET node or being a MANET node can communicate with IoT devices connected to the same and other MANET nodes in the same MANET or with cross-MANET over Internet connected IoT devices. A MANET connected IoT device can also communicate with IoT devices connected to Internet nodes, with IoT devices being Internet nodes with non-IoT MANET nodes, and with non-IoT Internet nodes. An IoT device connected to an Internet node or being an Internet node can communicate with IoT devices connected to MANET nodes, with IoT devices being MANET nodes, and with non-IoT MANET nodes.

Routing for IoT devices in an Internet connected MANET requires some MANET topology. The cluster topology proposed in [6] is for MANET nodes which are either IoT devices or controllers of connected IoT devices. Clusters are dynamically formed from MANET nodes within the wireless radio range, with each cluster then selecting a clusterhead (CH). MANET nodes which are not CH are cluster members with the closest CH within the radio range, while the number of CH can be different in different MANETs. Cluster members only communicate with each other and their nominated CH, which is responsible for transmitting, aggregating and in some cases, compressing data gathered from its cluster members.

TABLE I. COMMUNICATION OPTIONS FOR MANET CONNECTED IOT DEVICES

Communication Partner	Network Connectivity of an IoT Device			
	To a MANET node	*Is a MANET node*	*To an Internet node*	*Is an Internet Node*
An IoT device connected to a MANET node			x	x
An IoT device which is a MANET node			x	x
An IoT device connected to the same MANET node	x	x		
An IoT device which is the same MANET node	x			
An IoT device connected to another node in the same MANET	x	x		
An IoT device which is another node in the same MANET	x	x		
An IoT device connected to a node in another MANET	x	x		
An IoT device which is a node in another MANET	x	x		
A node in the same MANET	x	x		
A node in another MANET	x	x		
A non-IoT MANET node	x	x	x	x
A non-IoT Internet node	x	x		

III. ROUTING FOR IOT DEVICES CONNECTED TO MANETS

Routing for IoT nodes in MANETs and IoT devices connected to MANET nodes use MANET routing protocols. Several proposals for MANET routing protocols exist, with extensive surveys being provided in [8], [9], [10], [11], [12]. The IETF Routing Area Working Group on MANET [13] has proposed and evaluated Internet standards for MANET routing protocols.

IoT nodes in MANETs and IoT devices connected to MANET nodes have by definition IP connectivity with the Internet and the MANETs are typically LLNs. A proposed IPv6 connectivity standard for LLNs is the 6LoWPAN protocol [14]. The *Routing Protocol for Low-power and Lossy Networks* (RPL) has been proposed by the IETF Working Group ROLL WG [15] for LLN implementations based on 6LoWPAN. RPL is a distance vector IPv6 routing protocol. Routing paths consist of LLNs nodes organized as a set of destination oriented directed acyclic graphs (DODAGs). A DODAG typically consist of IoT nodes and a sink node which collects data from the IoT nodes. A typical networking architecture for LLN connected IoT devices is shown in Fig. 1. A backbone router interfaces RPL or other LLN routing with Internet routing when a LLN connected IoT device communicates with an Internet host or with some other IoT device than a device in the same LLN. [16]

MANET routing protocols are typically classified into proactive (table driven), reactive (on demand), and hybrid routing protocols. This classification is based on how mobile nodes acquire and maintain routing information. In a proactive protocol each mobile node maintains consistent and up-to-date routing information from each network node to all other network nodes. A reactive routing protocol establishes at least one available route but only when a route is needed. A hybrid routing protocol attempts to combine the advantages of both proactive and reactive routing approaches [9], [10], [17], [18].

MANET routing protocols have also been classified into uniform and non-uniform protocols. This classification is based on the roles of mobile network node in routing. All nodes have the same role, importance, and functionality in a uniform routing protocol, which is either proactive or reactive. Some mobile network nodes apply distinct management functions and/or routing schemes in a non-uniform routing protocol for which different classification schemes have been proposed as in [8] and [10].

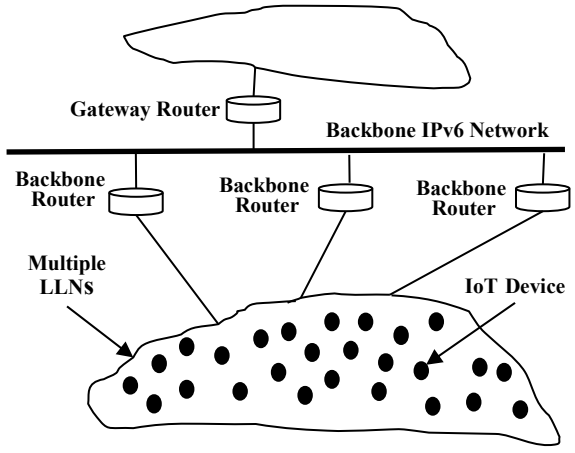

Figure 1. A network architecture for LLN connected IoT devices [19].

A mobility based routing protocol for cognitive radio enabled MANETs (CRMBR) has recently been designed to work with IoT devices. CRMBR has been comparatively evaluated with the established routing protocols AODV and DRS, by simulation experiments on an OPNET platform [20]. Throughput results for CRMBR are shown to be higher than AODV and comparable to DSR, while corresponding end-to-end delay analysis confirms CRMBR is significantly shorter than for DRS and even shorter than for AODV. Crucially however, security features for CRMBR are neither critically analyzed nor evaluated. [21]

IV. Threats and Vulnerabilities to Routing in MANETs

Security threats against routing in MANETs are classified into either passive or active attacks [22]. The purpose of a passive attack is usually to eavesdrop on routing communication and to retrieve information from monitored data packets. In a passive attack a malicious network node tries to identify communication parties and the contents of their communication. This can open up possibilities to launch further security attacks. The attack is passive since the normal network communication is not altered. In an active attack a malicious node tries to interrupt, disturb, and/or change the routing functionality in a MANET. Active attack examples include [23], [24], [25], [26]:

- Modification
- Impersonation
- Fabrication
- Wormhole and Blackhole
- Selfish behavior.

In [27], network routing attacks against RPL can be generally classed as those which aim to:

- Exhaust resources like energy, memory, and power.
- Disrupt the RPL network topology by, for example isolating sets of nodes.
- Disturb traffic via spoofing and deception.

A. Security Attacks against RPL and Countermeasures

An insightful review of security attacks against RPL and countermeasures is presented in [16]. Such attacks can be classified as either confidentiality and integrity attacks, or availability attacks as is shown by the examples in Table II. A malicious network node can disrupt route paths with selective forwarding of data packets. A lightweight heartbeat protocol to protect LLN connected IoT devices against selective-forwarding attacks by RPL has been implemented in [28]. In Sybil attacks, malicious network nodes use multiple cloned identities of legitimate network nodes to compromise routing by making them unreachable. Cloned node identities can be detected by keeping track of the number of instances of each node identity [28]. In a wormhole attack, two malicious network nodes forward routing packets between each other in order to disrupt both routing topology and traffic flow. Authentication is one possible countermeasure such as the Merkle hash tree [29]. In a flooding attack an IoT node is overloaded with network traffic in order to exhaust its battery power. A denial-of-service attack is similar to a flooding attack and the purpose is to make the attacked network node unavailable to legitimate network traffic. A node issues a DIS (DODAG Information Solicitation) message to get the RPL topology information before joining a LLN. In a DIS attack, malicious nodes repeats sending DIS messages to neighbor LLN nodes in order to generate control overhead and eventually exhaust the battery power in the attacked nodes [27]. A proposed countermeasure is routing path validation [30]. In a blackhole attack a malicious network drops all data packets which should forwarded in routing [27]. Black nodes in a LLN can be detected by SVELTE, which is an intrusion detection system for IoT nodes, designed and implemented to detect packet dropping nodes by analyzing routing path tropology [31]. In a neighbor attack a malicious LLN node disrupts routing by forwarding data packets without recording its IP in the packets to makes two network nodes that are not one hop away from each other believe that they are neighbor nodes [32]. A proposed countermeasure is routing path validation [30].

TABLE II. Classification of Attacks against RPL [16]

Attack	Attack Class	
	Confidentiality & Integrity	***Availability***
Selective forwarding	x	
Sybil attack	x	
Man-in-the-Middle	x	
Wormhole	x	
Flooding		x
Denial-of-Service		x
DIS attack		x
Blackhole	x	x
Neighbour attack	x	x

V. Methodologies to Secure Routing for IoT Devices in MANETs

Methods to secure routing for MANET-connected IoT devices have been classified into security enhanced routing protocols and trust models. These will now be briefly explored.

A. Security Enhanced Routing Protocols

Secure routing protocols for IoT systems are either originally insecure IoT routing protocols which have been extended with security measures, or protocols which have initially been designed to be secure. Security extensions of some MANET routing protocols are listed in Table III. The Confidant extension to DSR [33] and the TAODV extension to AODV [34], [35] are trust based, while all remaining security extensions in Table III are cryptographic. In [36] an experimental comparison of the cryptographic security extension SAODV and the trust based security extension TAODV to the reactive protocol AODV [37] is presented.

TABLE III. SECURITY EXTENSIONS OF SOME MANET ROUTING PROTOCOLS [21]

Routing Protocol	Characteristics	
	Protocol class	***Security Extensions***
DSR	Reactive	SQoS Route Discovery Ariadne Confidant
AODV	Reactive	CORE SAODV TAODV SAR
DSDV	Proactive	SEAD
OLSR	Proactive	SLSP
ZRP	Hybrid	SRP
Others	Reactive	SPREAD ARAN

Several novel proposals for secure MANET routing have focused on protection against specific routing attacks such as hidden and participative wormholes. Recent algorithms for trust-based extensions to the routing protocol AODV have been proven by simulations to provide guaranteed protection against certain wormhole types [38], [39]. Interestingly, given their flexibility and lightweight nature, these wormhole detection solutions are certainly extendible to other types of cross-MANET wormholes because of the very long traversal time through the wormhole in comparison to traversal times between nodes within the same MANET.

B. Trust Models

The following recommendations for secure IoT routing protocol design have been proposed in [16]:

- Secure route establishment [40]
- Self-stabilization [41]
- Effective malicious node identification system
- Lightweight computations [41]
- Location privacy.

Identification/rejection of malicious network nodes and secure route establishment are highly important research challenges in routing protocol design for MANET connected IoT systems. Many trust models for MANET connected IoT devices have been proposed but which combinations of a trust model with a security enhanced routing protocol provide the best overall security is still an open research challenge.

Security weaknesses in the current RPL protocol standard [15] are highlighted in [42]. No protection is specified against selective forwarding attacks, sinkhole attacks, black and gray hole attacks, and version number manipulation attacks. There is no description on how IoT device authentication and secure network connections could be implemented. A secure version of the RPL protocol standard is a significant research challenge due to the current rapid growth of LLN network connected IoT systems worldwide.

VI. RESEARCH CHALLENGES

The following recommendations for secure IoT routing protocol design have been proposed in [16]:

- Secure route establishment [40]
- Self-stabilization [41]
- Effective malicious node identification system
- Lightweight computations [41]
- Location privacy.

Identification/rejection of malicious network nodes and secure route establishment are highly important research challenges in routing protocol design for MANET connected IoT systems. Many trust models for MANET connected IoT devices have been proposed but which combinations of a trust model with a security enhanced routing protocol provide the best overall security is still an open research challenge.

Security weaknesses in the current RPL protocol standard [15] are highlighted in [42]. No protection is specified against selective forwarding attacks, sinkhole attacks, black and gray hole attacks, and version number manipulation attacks. There is no description on how IoT device authentication and secure network connections could be implemented. A secure version of the RPL protocol standard is a significant research challenge due to the current rapid growth of LLN network connected IoT systems worldwide.

VII. CONCLUSIONS

Secure routing for MANET connected IoT systems is not only an IoT security issue, it is also an important Internet security issue because of the large and rapidly growing number of such systems. Many proposals have been made for both security enhanced MANET routing protocols and trust models for MANET connected IoT devices but research is needed to find optimal combinations of these approaches to secure routing. For MANET connected IoT devices LLN is a network topology for which a routing protocol standard, RPL, exists. However, a security enhanced RPL specification standard is a significant challenge, since the current RPL specification lacks protection against several security attacks. Gateway routers connecting IoT devices in MANETs must be trusted and reliable interfaces for secure MANET routing protocols and secure Internet routing protocols. Although many proposals for secure MANET routing exist, none of these provides protection against all current and possible future security attacks [22]. Looking forward, it is likely a synthesis of current and future proposals for secure MANET routing protocols will be needed to enable protection against existing security attacks, while emerging MANET-connected IoT systems present an entirely different set of challenges which will mandate new and innovative solutions.

REFERENCES

[1] IEEE Standard for Information technology, Part 15.4; Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs), IEEE Computer Society, 2006.

[2] The ZigBee Specification version 1.0, ZigBee Alliance, 2007.

[3] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Personal Area Networks (WPANs), IEEE Standard 802.15.1, 2005.

[4] HART Field Communication Protocol Specification, HART Communication Foundation Std., 2007.

[5] Wireless Systems for Industrial Automation: Process Control and Related Applications, Standard: ISA 100.11a, International Society of Automation, 2011.

[6] R. Bruzgiene, L. Narbutaite, and T. Adomkus, "MANET Network in Internet of Things System," in Ad Hoc Networks, J. H. Ortiz and A. P. de la Cruz, Eds. Rijeka: InTech, 2017, doi: 10.5772/66408

[7] D. De Guglielmo, S. Brienza, and G. Anastasi, "IEEE 802.15.4e: a Survey," Computer Communications, vol. 88, pp. 1-24, 2016.

[8] L. M. Feeney, A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks, SICS Technical Report T99/07, Swedish Institute of Computer Science, Sweden, 1999, http://eprints.sics.se/2250/01/SICS-T--99-07--SE.ps.Z

[9] L. Qin and T. Kunz, Survey on mobile ad hoc network routing protocols and cross-layer design, Technical report SCE-04-14, Systems and Computer Engineering, Carleton University, Canada, 2004, http://kunz-pc.sce.carleton.ca/Thesis/RoutingSurvey.pdf

[10] C. Liu and J. Kaiser, A survey of mobile ad hoc network routing protocols, MINEMA (Middleware for Network Eccentric and Mobile Applications) Scientific Programme Report TR-4, Univ. of Magdeburg, Germany, 2005, http://www.minema.di.fc.ul.pt/reports/report_routing-protocols-survey-final.pdf

[11] S. Taneja and A. Kush, "A survey of routing protocols in mobile ad hoc network," International Journal of Innovation, Management and Technology, vol. 1, no. 3, pp. 279-285, 2010.

[12] N. Patel, A. Pawar, and N. Shekokar, "A Survey on Routing Protocols for MANET," International Journal of Computer Applications, vol.110, no. 11, pp. 5-7, 2015.

[13] Mobile Ad-hoc Networks (MANET), IETF Routing Area Working Group, 2018, http://datatracker.ietf.org/wg/manet

[14] Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Request for Comments (RFC) 4944, IETF, 2007, http://tools.ietf.org/html/rfc4944

[15] RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, Request for Comments (RFC) 6550, IETF, 2012, http://tools.ietf.org/html/rfc6550

[16] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.

[17] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 78-93, 2008.

[18] U. Singh, "Secure routing protocol in mobile ad hoc networks – A survey and taxonomy," Int. J. of Reviews in Computing, vol. 7, no. 2, pp. 9-17, 2011, http://www.ijric.org/volumes/Vol7/Vol7No2.pdf

[19] P. Thubert, Ed. "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4," draft-ietf-6tisch-architecture-14, IETF, April 25, 2018, https://tools.ietf.org/html/draft-ietf-6tisch-architecture-14

[20] OPNET Network Simulator, 2018, http://opnetprojects.com/opnet-network-simulator/

[21] Y. Sun, J. Bai, H. Zhang, R. Sun, and C. Phillips, "A Mobility Based Routing Protocol for CR Enabled Mobile Ad hoc Networks," International Journal of Wireless Networks and Broadband Technologies (IJWNBT), vol. 4, no. 1, pp. 692-703, 2015.

[22] J. Karlsson, L. Dooley, and G. Pulkkis, "Routing Security in Mobile Ad-hoc Networks," Issues in Informing Science and Information Technology, vol. 9, pp. 369-383, 2012.

[23] P. Tomar, P. K. Suri, and M. K. Soni, "A comparative study for secure routing in MANET," International Journal of Computer Applications, vol. 4, no. 5, pp. 17-22, 2010.

[24] T. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile ad-hoc networks," International Journal of Computer Applications, vol. 9, no. 12, pp. 11-15, 2010.

[25] N. Garg and R. P. Mahapatra, "MANET security issues," International Journal of Computer Science and Network Security, vol. 9, no. 8, 2009.

[26] D. Wang, M. Hu, and H. Zhi, "A survey of secure routing in ad hoc networks," in Proceedings of the Ninth International Conference on Web-Age Information Management WAIM '08, USA: IEEE Press, 2008, pp. 482-486.

[27] D. Sharma, L. Mishra, and S. Jain, "A Detailed Classification of Routing Attacks against RPL in Internet of Things," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 3, no. 1, 2017.

[28] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," International Journal of Distributed Sensor Networks, vol. 9, no. 8, 2013.

[29] F. I. Khan, T. Shon, T. Lee, and K.-H. Kim, "Merkle tree-based wormhole attack avoidance mechanism in low power and lossy network based networks," Security and Communication Networks, vol. 7, pp. 1292–1309, 2014.

[30] H. Perrey, O. Landsmann, O. Ugus, M. Wahlisch, and T. C. Schmidt, "TRAIL: Topology Authentication in RPL," in Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, ACM Press, 2016, pp. 59-64.

[31] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real time intrusion detection in the internet of things," Ad Hoc Networks, vol .11, no. 8, pp. 2661-2674, 2013.

[32] S. Parthiban, A. Amuthan, N. Shanmugam, and K. S. Joseph, "Neighbor Attack Detection Mechanism in Mobile Ad-Hoc Networks," Advanced Computing: An International Journal (ACIJ), vol. 3, no. 2, pp. 57-67, 2012.

[33] S. Buchegger and J.-Y. L. Boudec, "Cooperation of nodes fairness in dynamic ad-hoc networks," in Proceedings of the IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), IEEE Press, 2002.

[34] X. Li, M. R. Lyu, and J. Liu "A trust model based routing protocol for secure ad hoc networks," in Proceedings of Aerospace Conference, vol. 2, USA: IEEE Press, 2004, pp. 1286-1295, ISBN 0-7803-8155-6.

[35] A. M. Pushpa, "Trust based secure routing in AODV routing protocol," in Proceedings of 2009 International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), USA: IEEE Press, 2009, pp. 1-6.

[36] J. Cordasco and S. Wetzel, "Cryptographic vs. trust-based methods for MANET routing security," Electronic Notes in Theoretical Computer Science, Elsevier, vol. 197, no. 2, pp. 131-140, 2007, http://www.cse.msstate.edu/~ramkumar/cryptvstrust.pdf

[37] C. Perkins, E. Beldin-Royer, and S. Das, Ad hoc on-demand distance vector (AODV) routing, Request for Comments (RFC) 3561, IETF, 2003, http://tools.ietf.org/html/rfc3561

[38] J. Karlsson, L. S. Dooley, and G. Pulkkis, "A new MANET wormhole detection algorithm based on traversal time and hop count analysis," Sensors, vol. 11, no. 12, pp. 11122-11140, 2011, http://www.mdpi.com/1424-8220/11/12/11122/pdf

[39] J. Karlsson, L. Dooley, and G. Pulkkis, "A Packet Traversal Time per Hop based Adaptive Wormhole Detection Algorithm for MANETs," in Proceedings of the 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM'16), 2016, pp. 1-7.

[40] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures," in Proceedings of the 15th International Conference on Computer Modelling and Simulation (UKSim), 2013, pp. 693–698.

[41] D. Airehrour and J. Gutierrez, "An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing," in CONF-IRM 2015 Proceedings, Association for Information Systems AIS Electronic Library (AISeL), 2015, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1030&context=confirm2015

[42] A. Kamble, V. S. Malemath, and D. Patil, “Security Attacks and Secure Routing Protocols in RPL-based Internet of Things: Survey,” in Proceedings of the International Conference on Emerging Trends & Innovation in ICT (ICEI) , IEEE Press, 2017, pp. 33-39.