The Korea Academic Society of Digital Business Administration (KASDBA)
(사)한국디지털경영학회

APCICT-2018 Conference Program

Asia Pacific Conference on Information Communication Technology (2018 APCICT)

Asia Pacific Conference on Information Communication Technology
(APCICT-2018)
Kyungpook National University
Daegu, Republic of Korea, July 6-7, 2018

■ Date: Friday and Saturday, July 6~7, 2018,
09:30 – 17:00

■ Place: Building No. 4, College of IT Engineering, Kyungpook National University,
Daegu. Republic of Korea

■ Organizers:

KNU KYUNGPOOK NATIONAL UNIVERSITY

College of IT Engineering, Kyungpook National University

KASDBA
(사)한국디지털경영학회

The Korea Academic Society of Digital Business Administration (KASDBA)

KIDICO 재단법인 한국디지털융합진흥원 KOREA INSTITUTE OF DIGITAL CONVERGENCE

Korea Institute of Digital Convergence (KIDICO)

■ Sponsor:

한국중소기업협업진흥협회
Korea Small Medium Business Association

NIA NATIONAL INFORMATION SOCIETY AGENCY

dcvb DAEGU Convention & Visitors Bureau

Conference Program

APCICT-2018 – Conference Schedule

Date – Friday, July 6, 2018

Venue – Building No. 4, College of IT Engineering,
Kyubgpook National University, Daegu, South Korea

Time	Program	Place
09:30 –10:00	Registration	Building No.4 College of IT Engineering
10:00 –11:00	Presentation Session 1-1	Room No. 101
	Presentation Session 1-2	Room No. 104
	Presentation Session 1-3	Room No. 108
11:15 –12:30	Opening Ceremony	Room No. 101 Building No.4 College of IT Engineering
	Welcome Message 1. Prof. You-Ze Cho, Dean, College of IT Engineering 2. Changsu Kim, President of KASDBA	

	Digital Grand Award Best Paper Award	
	Invited Talk Dhananjaya Acharya, Annapurna Broadcast Media Pvt. Ltd., Nepal	
12:30–13:30	**Lunch Break**	
13:30 -15:00	Presentation Session 2-1	Room No. 104
	Presentation Session 2-2	Room No. 108
15:00–15:15	**Coffee Break**	
15:15 – 17:00	Presentation Session 3-1	Room No. 101
	Presentation Session 3-2	Room No. 108

Date – Saturday, July 7, 2018

Venue – Daegu City

10:00 – 17:00	**City Tour**	Daegu City

Guidelines for the Presenters

- All participants are requested to participate in the opening ceremony.
- Each speaker will receive 15 minutes of presentation time (10-minute PowerPoint presentation followed by a five-minute question and answer).

There is no specific PowerPoint template. Please bring the PPT in USB.

Presentation Session Details

Presentation Session 1-1, Advanced Technology & Theory Session Chair: Dr. Eunser Lee Place: Room No. 101 Date: Friday, July 6th, 2018 Time: 10:00 – 11:00
An Overview of Selective Forwarding and Wormhole Attacks in Healthcare IoT (Yazdan Ahmad Qadri, Arslan Musaddiq, Dae Wan Kim, Sung Won Kim)
An Overview of Interoperability Issues in Vehicular Cloud Network (Arslan Musaddiq, Yazdan Ahmad Qadri, Dae Wan Kim, Sung Won Kim)
Video Summarization: A Review on Different Approaches (Rafiq Muhammad, Dae Wan Kim, Gyu Sang Choi)
Review of Literature in the Context of the TAM Model (Maqbool Ahmad)
Reviewing the Studies of Unified Theory of Acceptance and Use of Technology (UTAUT) for M-Commerce (Shoaib Imtiaz)
Digital Convergence and its Economic Sentiments (Maqbool Ahmad, Shoaib Imtiaz)

Presentation Session 1-2, Web-Based Technology

Session Chair: Dr. Won Il Lee
Place: Room No. 104
Date: Friday, July 6th, 2018
Time: 10:00 – 11:00

Quality Selection System for Video Types in Deep Learning Based Adaptive Video Streaming
(Won Sic Kwon, Dae Gi Kim, Jong Won Bang, Jin Chael Woo, I Seul Kim, Sung Wook Jung, Kyung Shik Lim)

Semantic Separation of Vectorized Homographs with Word2vec
(Uk Hwi Kim, Dong Jin Bak, Jae Un Yi, Byeong Je Ryu, Seok Ju Go)

Building Semantic Web Services and Developing Hybrid Contents Trial Services
(Tae Young Kim, Sun Jae Park, Chan Jun Lee,
Eun Koo Jeon, Eunmi Jeung, Yongju Lee)

An Influence of E-learning Class Redesign on the Degree of Flipped Learning Operation
(Youngsang Kim)

Korea's Innovative Clusters and Development Strategies - focusing on the ‘loosely coupled’ cooperation between the Daedeok Innopolis and the Pangyo Technovalley
(Won Il Lee)

Presentation Session 1-3, Information Security and New Media

Session Chair: Dr. Hyun-Sook Ahn
Place: Room No. 108
Date: Friday, July 6th, 2018
Time: 10:00 – 11:00

Big Data Analysis on the Perception of Gifted Education for Information Security
(Jong Hyun Lee, Dae Wan Kim)

A Study on the Evaluation of Gifted Education Institution for Information Security
(Jong Hyun Lee, Dae Wan Kim)

Study on the Activation of Spatial and Spatial Space based on New Media Art
(Eun Ji Yang, Dae Wan Kim)

The Influence of Emotional Intelligence on Individual Creativity
(Boung-Ik Kim, Sun-Kyu Lee)

A Study on Agriculture User-Centered Mobile Marketplace UI / UX
(Sang Tae Kim)

Presentation Session 2-1, Communication System and Technology

Session Chair: Dr. Gyanendra Prasad Joshi
Place: Room No. 101
Date: Friday, July 6th, 2018
Time: 13:30 – 15:00

Adaptive Video Streaming based on Deep Learning
(Kwon Won Sik, Dae Gi Kim, Jongwon Jung, Woo Jin Chul, Kim Sysul, Chung Sung Wook, Hong Sung Jun)

Visual-MIMO for Software-Defined Vehicular Networks
(Tae-Ho Kwon, Jai-Eun Kim, Ki-Soo An, Rappy Saha, Ki-Doo Kim)

Energy and Delay Constrained Packet Transmission MAC Protocol for Wireless Sensor Networks
(Seong Cheol Kim)

Novel Frame Synchronization Scheme of Electric Vehicle Charging System Based on Power Line Communication
(Isaac Sim, Yu Min Hwang, Young Ghyu Sun, Jin Young Kim)

Application Of Machine Learning Techniques To Tweet Polarity Classification With News Topic Analysis
(Hoyeon Park, Hyeonjeong Seo, Kyoung-Jae Kim, Gundoo Moon)

Application Of Anfis-Pid Controller For Statcom To Enhance Power Quality In Power System Connected Wind Energy System
(Huu Vinh Nguyen, Hung Nguyen, Kim Hung Le)

Performance of Turbo Equalizer for Powerline Communication Systems with Deep Learning

(Yu Min Hwang, Young Ghyu Sun, Issac Sim, Jin Young Kim)

Presentation Session 2-2,Radio Frequency System and Devices

Session Chair: Dr. Bhanu Shrestha
Place: Room No. 104
Date: Friday, July 6th, 2018
Time: 13:30 – 15:00

Sliding Mode Control for Manipulator Robot with Elastic Link
(Mai Nguyen Hoang, Tuan Pham Minh)

An ROI-Based Lidar Sampling Algorithm In The Road Environment
(Thai K. Nguyen, Xuan Truong Nguyen, Hyuk-Jae Lee)

Iterative Approach for Performance Improvement of PLC systems
(Yu Min Hwang, Young Ghyu Sun, Issac Sim, Jin Young Kim)

Performance of EV Charging System with PLC Systems
(Issac Sim, Yu Min Hwang, Young Ghyu Sun, Jin Young Kim)

Interference Analysis of PLC Convergence System
(Young Ghyu Sun, Yu Min Hwang, Issac Sim, Jin Young Kim)

Coplanar QCA Adders For Arithmetic Circuits
(Nuriddin Safoev, Jun-Cheol Jeon)

Implementation Of Full Adder Using 5-Input Majority Gate
(Sarvarbek Erniyazov, Jun-Cheol Jeon)

Design Of Falling-Edge Triggered T Flip-Flop Based On Quantum-Dot Cellular Automata

(Young-Won You, Jun-Cheol Jeon)

Presentation Session 3-1, Advanced Computing

Session Chair: Dr. Ajaya Kumar Jha
Place: Room No. 101
Date: Friday, July 6th, 2018
Time: 15:15 – 17:00

Implementation of Mobile Smart Key System using the NFC Function of the Smartphone
(JuGeon Pak, BoRam Lee, MyungSuk Lee)

A Study on Lightweight Cryptography Algorithm for IoT based Bicycle Sharing System
(Larsson Bajracharya, Jongmun Jeong, Mintae Hwang)

CoAP Monitoring System Using Logical Grouping Technique
(JeongYun Kang, Nathali Silva, Kijun Han)

Improvement of the KCF Tracking Algorithm through Object Detection
(Jae-Wan Park, Sung Joong Kim, Youngjae Lee, Inwhee Joe)

UX Design for the Visually Impaired to Improve Health Information Accessibility
(Woo Jin Kim, Min Ji Kim, Il Kon Kim)

Novel Interference Mitigation Scheme for PLC Convergence System Based on Deep Learning
(Young Ghyu Sun, Yu Min Hwang, Issac Sim, Jin Young Kim)

Presentation Session 3-2, ICT Convergence

Session Chair: Dr. Woong Jo
Place: Room No. 108
Date: Saturday, July 6th, 2018
Time: 15:15 – 17:00

Development of Bio-Medical Detection Platform using IoT Technology
(Seok-Joo Koh, Jeon Min Jun, Lee Dae Kwan, Kwon Jun Hyeon, Cha Ye Baek, Young-Hee Lee)

Culinary Recipe Recommendation based on Text Analytics
(Jiheon Hong, Heejung Lee)

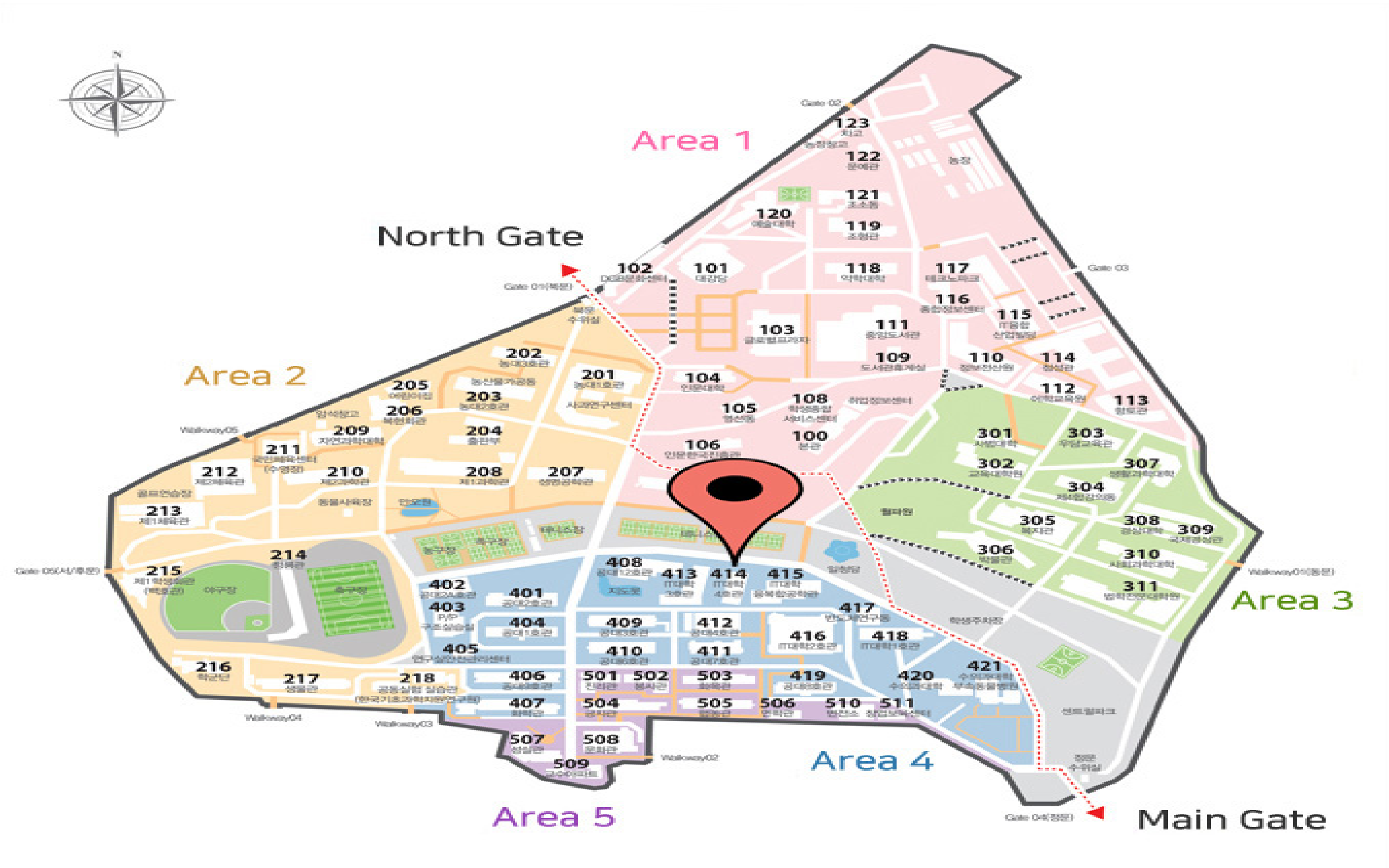
The Effect of External Technology Cooperation and Internal Relation on Innovative Behavior
(Won Il Lee)

The Influence Of Celebrity Endorsement On Consumer’s Attitude: A Study Case Of Smartphone Brands In Jakarta, Indonesia
(Ina Melati, Teddy Indira Budiwan, Haryadi Sarjono)

Dynamic Routing for HTTP Adaptive VBR Video Streaming Based on Software Defined Networking
(Thinh Pham Hong, Tan Tran Duc, Thinh Dang Truong, Truong Thu Huong, Nam Pham Ngoc, Alan Marshall)

Supply Chain Design of Potato Commodity in Wonosobo Regency, Central Java - Indonesia
(Haryadi Sarjono, Lim Sanny, Ina Melati)

Conference Venue Map



414. College of IT Engineering Bldg.4

Conference Venue: Building No. 4, College of IT Engineering,

Kyungpook National University, Daegu, Republic of Korea

Tel.: +(82) -10-3532-5295

Email: yongju@knu.ac.kr (Prof. Yong Ju Lee)

International Conference on ICT & Digital Convergence Business (ICIDB-2018)	APCICT-2018 Secretariat www.kasdba.org info@kasdba.org	KASDBA (사)한국디지털경영학회

An Overview of Selective Forwarding and Wormhole Attacks in Healthcare IoT

Yazdan Ahmad Qadri[a], Arslan Musaddiq[a], Dae Wan Kim[b], Sung Won Kim[a]*
[a]Department of Information and Communication Engineering, Yeungnam University, South Korea
[b]School of Business, Yeungnam University, South Korea
yazdan, arslan@ynu.ac.kr, c.kim,swon@yu.ac.kr

Abstract

The Internet of Things (IoT) revolution is allowing an explosive growth in the number of connected devices over the internet, especially in the field of medical monitoring. The network of sensors transmitting vital patient-generated data connected to each other constitute the healthcare internet of things or H-IoT. The Selective Forwarding attack and the Wormhole attack cause information deficit in the network and disrupt the routing paths of the patient-generated data respectively. Therefore, the need for security is paramount as ever increasing volume of sensitive medical data is transmitted over the internet. In this paper, we explore the threats faced by the body area networks due to Selective Forwarding attack and the Wormhole attack and we also study the counter-measures that are deployed against these attacks and identify their merits and limitations.

I. Introduction

A network of sensors and actuators associated with human bodies, which are connected together over a radio network is termed as a Wireless Body Area Network or WBAN. A typical WBAN follows a three layered architecture [1]. The first layer is the sensor or the device layer. It consists of wearables or implants that can measure physiological data called Patient-Generated Data (PGD). These sensors are connected to a Base Station (BS) [2]. Between the first and BS, Bluetooth Low Energy (BLE), ZigBee and Wi-Fi are the most popular communication technologies used to transmit data from the end devices to the BS. The PGD is received at the base station from the sensors and is then sent for storage and processing. The second layer is constituted by a long range link that connects the gateway to the cloud or the servers. Low Power Wide Area Network (LoRaWAN), Sigfox and Narrowband (NB-IoT) are used in this layer [3]. The PGD is then sent over to the third layer, the cloud or servers for storage and analytics. The analytics help in the modeling of physiological processes in the human body and diagnosis [4].

The communication between the three layers is secured by the use of security protocols. However, there are loopholes and vulnerabilities that can be exploited to listen to PGD without authorization, interrupt the data stream, introduce malicious data or even bring the entire system down. Selective Forwarding attack is one such threat that is responsible for creating information deficit in the network by dropping selective data packets during transmission. Similarly, Wormhole attack tries to disrupt the transmission routes by creating unauthorized links within a network. Therefore, it is necessary to secure the network from such threats.

The rest of the paper is organized as follows. The Selective Forwarding and Wormhole attacks and the appropriate counter-measures are discussed in section II. Section III explores the limitations of these countermeasures and future research directions. Section IV concludes the paper.

II. Security Challenges

The transmission or the network layer of the H- IoT architecture is responsible for the transmission of data from sensors to the cloud or servers. At this layer, there are a number of threats that can undermine the authenticity and integrity of the data. The two major attack types at the network layer are, 1) internal attacks and 2) external attacks. The internal attacks affect the nodes from within the network, either a legitimate node is compromised or a malicious node is introduced that has internal information about the network. On the other hand, external attacks are launched from outside the network where the attacker has no internal information about the network. [5]

Tomić et.al [6] identified various threats and their mode of operation at the different layers of the IoT network. Selective Forwarding attack operates by filtering the data packets from certain nodes while allowing data from other nodes. However in the Black Hole attack information deficit is created by dropping all the packets coming into the node. Wormhole attack creates an unauthorized link between two malicious nodes at different locations in a network

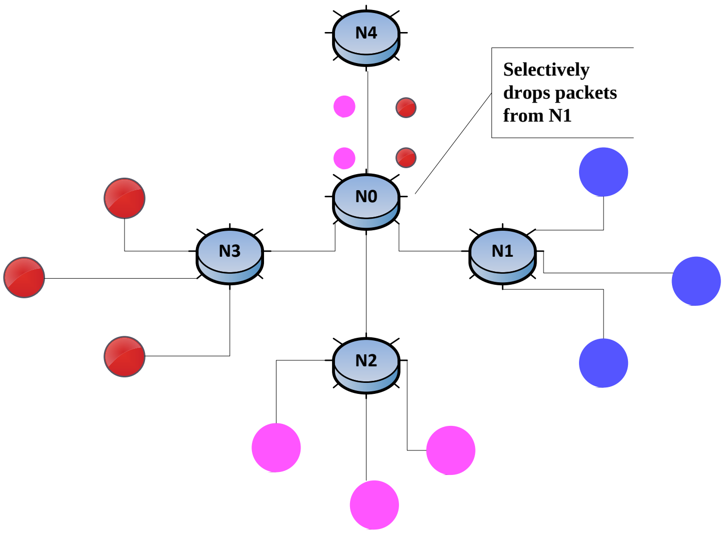


Figure 1. Operation of Selective Forwarding Attack

and sends data to the undesirable destination node. In this paper, we focus on the Selective Forwarding and the Wormhole attacks, which are internal threats at the network layer. These attacks are hard to detect as their affects can be similar to network disruptions caused by factors like poor channel, link quality, and node failure or even energy constraints. The overall performance of the network is degraded by the erroneous routing decisions. There is an increased threat of compromising the highly sensitive patient-generated data during these two attacks. The Wormhole attack has been observed to accompany other attacks [7], thus, its detection could help in securing the network from a range of network layer attacks too. In this paper we explore some of the most recent works in this direction.

a. Selective Forwarding Attack

The Selective Forwarding attack (SFA) involves the dropping of certain packets from the selective internal nodes. When a node drops all the packets, it is termed as a Black Hole attack. Figure 1 depicts the SFA operation. SFA is difficult to detect as there can be a number of reasons for the packet dropping such as an unreliable channel or medium access collisions, hence, careful analysis is required for the detection of SFA. The malicious node can selectively forward packets with reliability, therefore suppressing the suspicion about the errors in routing. Several measures have been presented for the detection and mitigation of SFA by using different features of an IoT network.

1. *Multi Approach Mechanism:* Mehetre et al [8] propounded a protocol that computes a secure and trusted route from source to destination for the WSNs. It is founded on three principal steps viz. detection of malicious nodes, securing the packets and finding a secure route. The use of Detection Packet (DP) for node detection is coupled with trust mechanism. Then, a dual assurance scheme is employed which includes a Selective Forwarding-based packet validation, and the data from the source node is encrypted using the elliptic curve cryptography (ECC) in order to make the forwarded data packet secure. A secure routing path is identified in the entire path transmission using the trust path selection, and Cuckoo Search (CS) algorithm. This algorithm provides an energy efficient and reliable counter-measure against SFA attack. The comparative analysis showed a satisfactory performance, but the latency incurred was not suitable for healthcare applications which essentially should be minimal.
2. *Acknowledgement Based Approach:* Liu et al. [9] proposed a Per-Hop Acknowledgement (PHACK) based detection scheme for SFA, which can effectively detect the attack and additionally recover from the attack. In this scheme, each intermediate node along a forwarding path is responsible for sending acknowledgement packets (ACK) to the source node for each packet received. The confirmation information is sent to the sink node via different paths to avoid single path failure. This method is also able to identify the suspect nodes and removing them from the routing path. The routing path is reorganized and packets are resent in a bid to recover the lost data. This method has an improved detection accuracy but makes no improvement in energy efficiency of the network hotspots. The simulations have shown an increase in energy use at the periphery of the network. Additionally, this scheme is not suitable for mobile WSN's like in case of H-IoT.
3. *Rule Based Approach:* Alajami et al. [10] presented a rule based intrusion detection system (IDS) to detect the SFA. The system has three layers viz. (1) Data Receiving Layer which stores the information required for rule processing; (2) Rule Processing Layer is used for matching the information with the applicable rules; (3) The Detection Layer makes the routing decisions based on the information from the above layers.

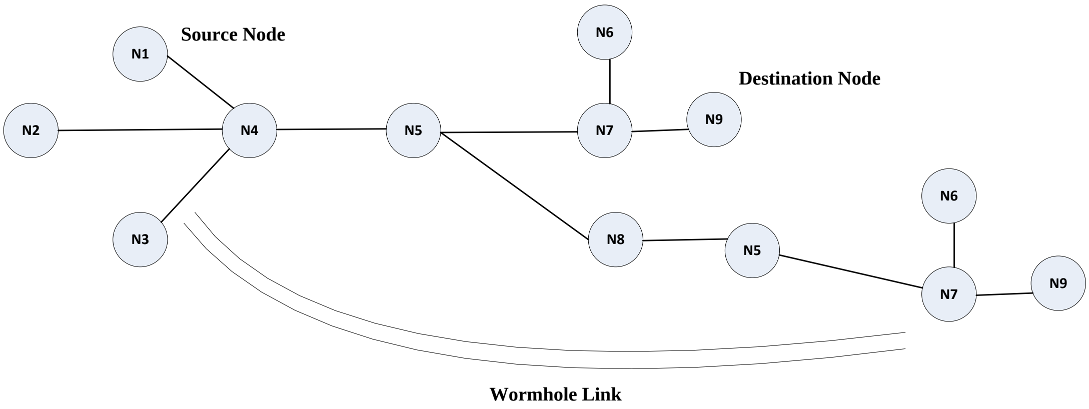


Figure 2. Wormhole Attack in a Network

This approach uses low energy and computational resources, however, it is not suited for detecting dynamic attacks which are adaptable to the network security mechanisms.

b. Wormhole Attack

A Wormhole attack is a passive nature attack which creates a malafide link between two points, usually to the malicious node, within the network. Wormhole attack creates a shortcut between source and destination by creating, either a high-quality wireless out-of- band link or a wired link for the construction of Wormhole tunnels [22] as shown in Figure 2. If an attacker is able to execute a Wormhole attack, there is a high probability that malicious nodes can use it for traffic analysis or cause a Denial-of-Service (DoS) attack by dropping certain data or control packets [17].

1. *Probability Based Approach:* The Wormhole Resistant Hybrid Technique (WRHT) has been proposed by Singh et al [11]. It combines the use of Watchdog algorithm and Delphi method to detect the presence of a Wormhole attack. WHRT is considered as an offshoot of the Ad-hoc On Demand (AODV) routing protocol. During the route discovery phase of AODV, time delay probability per hop is calculated and using this time delay probability for the complete path is calculated. The per hop time delay probability (TDP_H) is measured to further calculate time delay probability (TDP_P) for the complete path. Then packet loss probability per hop is calculated and also the packet loss probability for the complete path. These values are used to determine if a Wormhole link exists or not. This approach has been found highly effective against Wormhole attack with a better detection accuracy
2. *Modified AODV*: Amish et al. [12] postulated a modified version of the AODV protocol called Ad-hoc On-demand Multipath Distance Vector (AOMDV) routing protocol which detects the multiple paths that exist between two nodes. The sender nodes sends a request (RREQ) packet to the destination node from a known route in the routing table. If no route is present, the sender broadcasts it. As a reply, the response (RREP) packet is received by the sender via multiple paths that exist between the two nodes. To detect the malicious path or the wormhole, the node calculates the round trip time (RTT) and a threshold RTT value to compare the reliability of different paths. This method can be applied in mobile WSN’s but have a large computational overhead.
3. *Range Free Localization Methods:* García-Otero et al [13] put forth two counter-measures against the wormhole attacks using range free localization scheme. The novel approaches postulated use the “sensor localization with ring overlapping based on comparison of received signal strength indicator” (ROCRSSI) algorithm. The first method detects and localizes the Wormhole node simultaneously. The second approach tries to localize the Wormhole node post detection. The simultaneous detection and localization approach involves calculation of the location and Received Signal Strength (RSS) by the unknown-location nodes based upon the information broadcasted by the anchor nodes via beaconing packets. The node is able to decide the real distance from each anchor node by applying a monotonicity constraint. The unknown-location node computes the endorsements from each cell in its periphery to determine if it wants to join the network. In the localization post detection approach, the similar process is carried out with the roles reversed. The tested node broadcasts its information to the anchor nodes so that the anchor nodes calculate the RSS values. The verification is positive if the RSS values are consistent with the advertised position. The

decision node gives a decision based on the number of discrepancies at each anchor node which should be less than the threshold value. This approach is very accurate if a large number of anchor nodes are present. The shadowing effects prove detrimental to the accuracy of this approach.

III. Limitations and Future Scope

The methodologies discussed in the section II face some drawbacks. The requirements of H-IoT include low latency and low overhead due to its critical nature. Therefore, we identify and highlight these weaknesses. Table 1 presents the summary of the counter-measures discussed in the preceding sections and also provides an insight into the limitations of these countermeasures. The current techniques usually have limited effectiveness in large networks. Since, H-IoT concept is aimed for large scale deployment, the current methods face issues like large delay and increased packet drops when deployed in large scale scenarios. There is a need to develop methods suited for a large scale deployment. The nodes deployed are usually low on computational power due to energy constraints. Therefore, low overhead incurring methodologies need to be explored. Active Detection Methods (ADM) or real-time operation should be developed for ever evolving security threats that are adapting to the new network scenarios. Needless to say, the energy efficiency needs be improved by introducing low computational methodologies. One of the primary requirements is the reduction of latency as H-IoT is a time critical system.

IV. Conclusion

H-IoT constitutes a network of body sensors which transmit the physio-chemical data of the body over the internet. The data being sent is highly sensitive and is prone to a multitude of attacks. Therefore, in this paper we reviewed the conceptual working of the Selective Forwarding and Wormhole attacks, their significance and the counter-measures deployed to tackle these attacks. Each counter-measure is weighted for its advantages and the limitations. The need for security in such networks is critical and thus, the highlighted limitations invite a need for novel and effective solutions. Finally, we presented the open research issues and future directions pertaining to the mitigation of Selective Forwarding and Wormhole attacks.

Table 1: Countermeasures and their limitations against Selective Forwarding and Wormhole attack

Attacks	References	Key Concept	Significance	Limitations
SF	Mehetre et al. [8]	• Three tier approach, detection of malicious, securing the data using ECC & packet validation and secure routing using CS algorithm.	• High performance and energy efficiency.	• Latency not optimized for Healthcare IoT.
	Liu et al. [9]	• Per-Hop Acknowledgement (PHACK) based detection and recovery.	• Good detection accuracy. • Recovery of lost packets.	• Not suitable for mobile WSN's • Energy efficiency needs improvement.
	Alajmi et al. [10]	• Rule based Intrusion Detection System (IDS)	• Low storage requirements. • Energy saving ability.	• Not suited for dynamic attacks.
WH	Singh et al. [11]	• The Wormhole Resistant Hybrid Technique (WRHT) is implemented.	• Highly promising detection accuracy and can be used with any routing protocol.	• Effectiveness against multiple wormhole channels is not established. • Complex calculation required.
	Amish et al. [12]	• Modified AODV protocol top detect multiple paths called AOMDV	• Improved throughput.	• High computational overhead. • Reduced Packet Delivery Ratio.
	García-Otero et al [13]	• ROCRSSI based Wormhole localization and detection.	• High detection accuracy. • Simultaneous detection and localization approach as well as localization post detection approach is presented.	• Not effective under shadowing effects. • Accuracy depends on number of anchor nodes.

References

[1]. M. R. K. Naik and P. Samundiswary, Wireless body area network security issues-Survey, International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), (2016).

[2]. D. He, S. Zeadally, N. Kumar and J. H. Lee, Anonymous Authentication for Wireless Body Area Networks with Provable Security, IEEE Systems Journal. vol. 11, 4 (2016), 1-12.

[3]. S. Baker, W. Xiang, and I. Atkinson, Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities, IEEE Access, 5 (2017), 26521-26543.

[4]. F. Firouzi, B. Farahani, M. Ibrahim, and K. Chakrabarty, From EDA to IoT eHealth: Promise, Challenges, and Solutions, IEEE Trans. Comput. Des. Integr. Circuits Syst. 70 (2018), 1- 16.

[5]. A. Salleh, K. Mamat and M. Y. Darus, Integration of wireless sensor network and Web of Things: Security perspective, 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam. (2017), 138-143.

[6]. I. Tomić and J. A. McCann, A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols, in IEEE Internet of Things Journal. vol. 4, 6 (2017) 1910-1923.

[7]. S. Goyal, T. Bhatia and A. K. Verma, Wormhole and Sybil attack in WSN: A review, 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi. (2015), 1463-1468.

[8]. D. C. Mehetre, S. E. Roslin, and S. J. Wagh, Detection and prevention of black hole and Selective Forwarding attack in clustered WSN with Active Trust, Cluster Computing, 2018.

[9]. A. Liu, M. Dong, K. Ota and J. Long, PHACK: An Efficient Scheme for Selective Forwarding Attack Detection in WSNs, Sensors, vol. 15, 12 (2015), 30942-30963.

[10]. N. M. Alajmi and K. M. Elleithy, Selective forwarding detection (SFD) in wireless sensor networks, 2015 Long Island Systems, Applications and Technology, Farmingdale, NY. (2015), 1-5

[11]. R. Singh, J. Singh, and R. Singh, WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks, Journal of Mobile Information Systems, vol. 2016 (2016) 1-13.

[12]. A. Parmar and V.B. Vaghelab, Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol, Procedia Computer Science, vol. 79, (2016) 700 – 707.

[13]. M. García-Otero and A. Población-Hernández, Detection of wormhole attacks in wireless sensor networks using range-free localization, 2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona. (2012), 21-25.