Conference Proceedings of The Kabarak University International Conference on Computing and Information Systems, Edited by Christopher M. Maghanga and Moses Thiga. 14th-15th October 2019 Nakuru, Kenya.

Weaknesses and Security Obstacles in The Application of MANETs for Provision of Smart Health Care

Kirori Mindo [1] , Moses M Thiga [2] , Simon M Karume [3]
Department of Computer Science and Information Technology, Kabarak University, Kenya
[1]Tel: +245721864816. Email: kirori@kabarak.ac.ke
[2]Tel: +254720780468, Email: mthiga@kabarak.ac.ke
[3]Tel: +245722499397, Email: smkarume@laikipia.ac.ke

Abstract

The use of smart devices in provision of healthcare provides numerous benefits. Use of technology in the healthcare profession has generally led to faster diagnosis, lower costs, health workers and research collaboration, reliable services, efficient and effective healthcare systems as well. The provision of smart healthcare services is dependent on MANETs. While technology is particularly indispensable, security of the systems and data remains a critical challenge that hinders the accelerated adoption of smart health care. It is reported that smart healthcare devices experience twice the number of cyber security attacks as opposed to other industries. These attacks and are made possible due to the weaknesses and nature of smart devices in MANETS. These weaknesses give rise to security obstacles that inhibit the adoption of smart health care. There is need to investigate these weaknesses and obstacles in the application of MANETs for provision of smart health care. This study will describe and enlighten the various obstacles so as to aid guide on the best practices for provision of secure Smart Healthcare. This research used a desk research of general literature review methodology. The results identify the various weakness and outline commensurate vulnerabilities as well as attacks that take advantage of these vulnerabilities. Ultimately this research gives design recommendations that can be incorporated in providing ways to seal these gaps.

Keywords: MANET, Smart Heath Care, IOT, DDos, Cyber Attacks.

1. Introduction

It is reported that smart healthcare devices experience twice the number of cyber security attacks as opposed to other industries. FortiGuard Labs that provides cyber security defence mechanisms reported that healthcare experienced an average of 32,000 intrusion cyber security attacks per day in 2017. This is in comparison to 14,300 attacks in other industries (Adefala, 2018). A recent cyber-attack regarded as the biggest distributed denial-of-services attack ever experienced, a botnet of thousands of hacked IOT smart devices redirected traffic to a European based webserver in 2018 with packets exceeding one terabit per second (Liu, Jin, Hu, & Bailey, 2018).

It was recently reported by Ars Technica (Urquhart & McAuley, 2018) that hackers wrestled control over various IOT devices including cameras, routers and other IOT devices and initiated several DDoS attacks, which propagated data exceeding 300 Gbps In 2014, a children's Boston Hospital was a victim of a consistent DDoS attack, whereby hackers against Justina Pelletier at that time withheld at the hospital in Boston against her parents' wishes, were seeking her release. (Hongach, 2018). Recently an NSA cyber weapon - WannaCry was spread across the world, it infected several 200,000 Windows based

machines which included systems at more than 45 hospitals in the United Kingdom. Various medical devices and technology-based healthcare devices were affected too, Forbes has learned (Kao & Hsiao, 2018). Orangeworm hackers have also been recorded to have attacked X-Ray and MRI Machines by targeting critical systems executed by major international health companies based in the United States, Europe, and Asia with a key focus on the healthcare devices (Arapi, 2018).

2. The Problem

Security of smart healthcare devices that provide mission critical support in healthcare is extremely vital. These devices, which run on MANETs, are such that their physiognomy lacks the adequate capability to devise robust systems to shield themselves against eavesdropping, malicious attacks, packet sniffing and other security threats. There is a great need to dissect and expound on these weaknesses and vulnerabilities that creates obstacles limiting the uptake of smart devices in healthcare.

3. Methodology for the Identification of Existing Weaknesses and Security Obstacles in The Application of MANETs For Provision of Smart Health Care.

A literature review study was carried out to examine and identify the weaknesses and security obstacles in the application of MANETs in the provision of Smart Health. The following were the objectives of the literature review;

i) To identify weaknesses if any, within the MANET ecosystem as a consequence of the device(s) physiognomy.
ii) To identify the various risks and attacks that can happen or be experienced within the MANET ecosystem as a result of the weaknesses identified.

The literature review was premised on the following empirical research questions.

- To what degree do the weaknesses within a MANET ecosystem contribute to vulnerability?
- To what extent does the weaknesses of MANET devices and the ecosystem, contribute to risks and expose the devices, data and network to attacks.
- To what magnitude do the various weaknesses contribute to loss of confidentiality and availability of the devices and/or data?

4. Literature Review.

The following some of the common attacks in internet of things as presented by various authors

i. Leakage of Information (Confidentiality)

Data and information collected and transmitted by the smart devices within an MANET wireless sensor network is susceptible to leakage. Data and information from these devices is easily leaked since there lacks sufficient data encryption that is applied either between gateway and sensors or between the sensors themselves. In addition, user authentication to prevent un-authorized access and/or enable detection of unwanted and unauthorized parties is often weakly implemented (Rath et al, 2018).

ii. Denial of Service and/or Distributed Denial of Service (Availability)

This is a common attack that denies users from accessing the system(s) and information when and if they require it. This DOS/DDOS attack targets a device by using malicious unwanted response requests thereby draining resources and rendering the device unable to respond to genuine user requests. While no data is leaked or exposed, it is very disastrous as it makes systems unusable and

renders data/information un-useful as a result for the period of the attack (Dhindsa and Bhushan, 2019).

iii. Falsification (Integrity)

This attack happens when a wireless device is in communication with the gateway and the attacker successfully captures the collect packets in transition and alters the fields containing routing information. As a result, the attacker can access the information therein and alter, leak or destroy the data/information as a whole. Most SSL mechanisms have the capability to protect against this type of attack, while unauthorized devices that gain access should be entirely blocked. Most of these attacks happen as passive eavesdropping and/or traffic analysis. Hostile silently listen the communication (Ngomane, Velempini and Dlamini 2018).

5. Research Methodology for Identifying the Weaknesses and Security Obstacles in the Application of MANETs for Provision of Smart Health Care.

The literature review study exposed numerous weaknesses that hinder adoption of MANETs in healthcare due to the nature of these devices and their physiognomies. The results identified the security weaknesses in MANETs that have inhibited rapid adoption in smart devices for provision of healthcare, as follows.

i. Weakness 1: Distributed Operation

One of the characteristics of MANETs is that they have no centralized control of network operations. This lack of coordination can bring addressing conflicts, routing and data loops. This results from the lack of a well-coordinated defence mechanism as shown (Inzillo, Serianni and Quintana, 2019)

ii. Weakness 2: Multi-Hop routing

Devices in MANETs forward packets via an intermediate node thus bringing up possibility of eavesdropping and man in the middle attacks. Due to their mobile nature, a device that requires to remotely forwards packets to a neighbouring hopping device, which can turn out to be a malicious device, or one that is not authorized to handle the traffic (Zhang et al., 2018).

iii. Weakness 3: Light Weight Terminals

These devices in MANETs are considered Light Weight Terminals with Low CPU capability, low power storage and small memory size. Thus they do not have the ability to provide robust security and protection. Low CPU capability translates to their inability to run high key security algorithms. Low power storage is a weakness that can cause the device to deplete its power resource once overworked by malicious attacks. In addition, its small memory size incapacitates it from running robust security systems (Kamakshi and Kumar, 2018).

iv. Weakness 4: Shared Physical Medium

MANETs ecosystem is by nature a wireless shared medium propagated by CSMA/CA for purposes of collision avoidance due to the shared nature of the physical medium. These devices are thus visible to other devices on the same channel and or any devices with

sniffing capability. Further, attacks like MAC addressing snooping are easily propagated in such an environment (Kamakshi and Kumar, 2018).Results.

v. Weakness 5: Limited bandwidth

Devices in MANET ecosystems mainly exhibit a small packet data size, which propagates bandwidth with a data rate of upto 250kbit/s. This is quite limiting as compared with other devices as those on Wireless Fidelity. This also means that a large case of DDOS on such an ecosystem can easily clog the network (Delkesh and Jamali, 2019).

vi. Weakness 6: Dynamic topology

There is a rapid and dynamic topology change, due to the mobility of the devices in MANETs. This brings upon disturbed trust among nodes, due to their reconfiguration and reorientation to new networks and unfamiliar intermediary devices (Chaudhary and Shrimal, 2019).

vii. Weakness 7: Routing Overhead

Intermediary devices within the MANET ecosystem experience a lot of routing information overhead due to the dynamic networks and mostly stale routes. There are also numerous and unnecessary routing overhead as a result which clog and slow up route resolution functionalities (Garikipati and Rao, 2019).

viii. Weakness 8: Hidden terminal problem

The hidden terminal problem is a common phenomenon which multiplies transmissions thus resulting to collision of packets in some cases. This hidden terminal can also lead to packet losses due to transmission errors. Collisions and packet losses especially in UDP communication are considered expensive since UDP is an un-reliable protocol without strategies for recovery in data loss (Tomar et al., 2019).

ix. Weakness 9: Wireless Radio

Devices in MANETs communicate over wireless links thus suffer from electro-magnetic interference, uni-directional links and frequent path breaks due to mobility of nodes which can lead to loss of data or duplicate frames. (Das and Pal, 2019).

x. Weakness 10: Mobility

By the fact that they have dynamic mobility, this nature brings about induced route changes and frequent route changes which can cause data loss. This would have dire consequences especially when this technology is applied to monitor healthcare for users whom their lives depend on monitoring devices (Fatima et al., 2019).

xi. Weakness 11: Battery constraints

Most MANET devices rely on batteries to provide power. If the device experiences DDOS attacks, it can lead to draining of battery resources and thus result to broken links or dead links which lead to data loss (Singh et al., 2018).

xii. Auxiliary Security Weakness

The nature of these devices in MANETs is auxiliary node cooperation which can lead to exposure to numerous security attacks. Devices are required to first corporate with similar devices within the ecosystem, while cautious connectivity is discouraged. As a result, a device looking to gather reconnaissance data, finds cooperative devices (Aldaej, 2019).

6. Results.

The table below summarises the identified weaknesses and vulnerabilities through which various threats take advantage of to attack the MANET.

Table 1: Summary of MANET Vulnerabilities that propagate security threats.

No	Weakness	Vulnerability	Attack / Risk /	Source
a)	Distributed Operation	No centralized control of the network operations	Each node is a relay	(Inzillo, Serianni and Quintana, 2019)
b)	Multi-Hop routing	Packets forwarded via an intermediate node	Eavesdropping	(Zhang et al., 2018)
c)	Light Weight Terminals	Low CPU capability, low power storage and small memory size	Non-Robust systems	(Kamakshi and Kumar, 2018)
d)	Shared Physical Medium	Wireless communication	Medium accessible to other entities	(Kamakshi and Kumar, 2018)
e)	Limited bandwidth	Lower capacity	Lower throughput	(Delkesh and Jamali, 2019)
f)	Dynamic topology	Rapid Topology change	Disturbed trust among nodes	(Chaudhary and Shrimal, 2019)
g)	Routing Overhead	Dynamic networks	Stale routes and unnecessary routing overhead.	(Garikipati and Rao, 2019)
h)	Hidden terminal problem	Multiple transmissions	Collision of packets Packet losses due to transmission errors High packet loss	(Tomar et al., 2019)

i)	Wireless Radio	EMI interference	Uni-directional links, frequent path breaks due to mobility of nodes.	(Das and Pal, 2019)
j)	Mobility	induced route changes	Frequent route changes which can cause data loss.	(Fatima et al., 2019)
k)	Battery constraints	Restricted power source	Lack keep alive	(Singh et al., 2018)
l)	Auxiliary Security threats	node cooperation	Exposure to numerous security attacks.	(Aldaej, 2019).

7. Validation of the Results.

Following the general literature review on security weaknesses in the application of MANETs for the provision of Smart Health care, there was need to perform validation of the results recorded above, to ascertain that malicious attacks like DDOS do happen on MANETS easily. This section was achieved through using Proof of Concept methodology.

The main objective of this section was to interrogate whether, by taking advantage of weaknesses in MANETs, the following activities can be achieved;

j) To verify if a DDOS can be easily propagated within a MANET.

k) To verify if a Blackhole attack can be carried out within a MANET.

A MANET network was implemented on Linux, to review the performance of devices so as to validate and ascertain the results of the desk research. This network was setup without any intrusion detection scheme implemented so as to note and review the weaknesses that can cause loss of confidentiality, availability and integrity thus inhibit the application of MANET for provision of smart health care. The Figure 4 below shows the MANET set up without any security IDS and the various malicious attacks that were experienced.

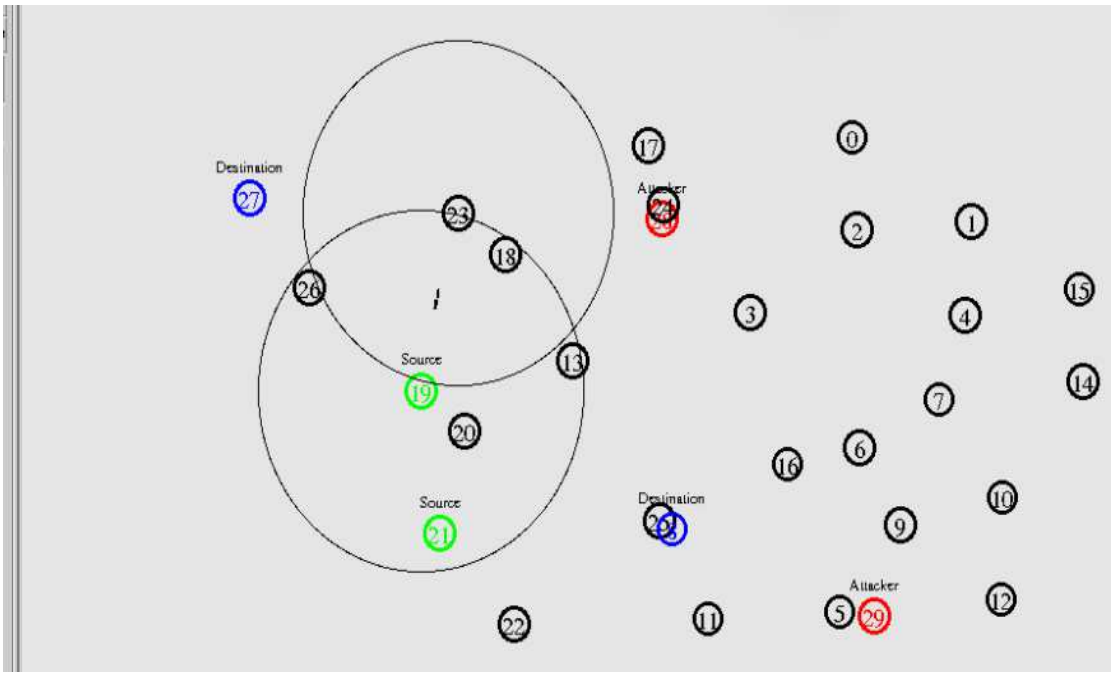

Figure 1: An open vulnerable MANET

The various devices in the above network propagated data using Bluetooth, with two source (19 and 20) and two destination devices (26 and 27). Two other devices were configured as malicious nodes which are required to propagate DDOS and blackhole attacks on the MANET.

Running the network above, the experiment enabled the deployment of two types of malicious data in DDOS and blackhole attacks, which were feasible and that run successfully. As a result, there was a high propagation of duplicate packets on the network. This is extremely dangerous, since an attacker can take advantage of this gap and launch data interception, man in the middle attacks, packet replay as well as packet delay.

Following the ability to propagate these attacks, the experiment above confirms that, if replayed in a real-world environment, it can have serious ramifications to healthcare users. These includes and especially those ailing patients with heart beat monitors, pacemakers, blood pressure monitors can bring life threatening consequences. Table 4 below shows the various malicious packets that were successfully permeated and their anomalous characteristic.

Table 2: Malicious Packets permeated into the MANET successfully.

No	Data Type	Disposition	Vulnerability	Attack
1	ICMP	High Rates	DDOS	Availability
2	TCP	Black hole	Reconnaissance	Confidentiality

Table 4 above, shows that MANETs are vulnerable and thus propagate two types of attacks against confidentiality and availability as shown above by Blackhole and DDOS attacks. Blackhole attacks on a network, can affect the data in two ways;

- A malicious node transmits an erroneous RREP (Route Replay) message to the source device; masquerading as the shortest path to the destination thus packets are forwarded to the malicious node.
- In another scenario, incoming or outgoing traffic can be redirected to a blackhole (or a dev/null) without the source device knowing that the traffic did not reach its intended destination

In both cases above, a third party can receive unauthorized or unsolicited packets leading to both loss of confidentiality and/or availability of data. DDOS can be disastrous since systems, data or routes can be completely unavailable to devices, people or systems that direly need them.

8. Recommendations.

Subsequent to the validation of general literature review on security weaknesses and obstacles in the application of MANETs for the provision of Smart Health care, there emerged observable and feasible recommendations which are enumerated below. The resulting design would take cognizance of the weaknesses in IDS systems for MANET and ensure that MANETs design should not introduce a window for added vulnerabilities to the system and should be self managed to monitor and identify both hardware and software abnormalities and modifications spontaneously. The following are key areas to apply when designing a secure IDS system for MANETs.

- The Smart MANET IDS should have ability to identify intrusions by taking cognizance of unfamiliar device addresses;
- The Smart MANET IDS should not permit TCP sessions that are initiated by devices outside its network to get into fruition;
- The Smart MANET IDS should detect the intrusions with low processing and communication overhead;
- The Smart MANET IDS should identify scenarios that cause high resource usage in CPU, Ram and bandwidth within the ecosystem;
- Dynamic network topology and mobility of MANET devices should not affect the detection accuracy of the Smart IDS MANET system;

Conclusion.

This paper discussed the literature review on weaknesses that inhibit application of MANETs for smart health. The literature provided vital knowledge on various other researchers' experiences that will guide the design, implementation and evaluation of a fused machine learning intrusion detection model for the provision of smart health care in MANETS.

The results showed that existing intrusion detection methods are mainly built for compute-intensive systems and mainly and most commonly, for networks with a rigid architecture and topology. MANET are mobile and deployed in a scattered fashion, with a frequent change in network topology which translates from their continuously changing

addresses schemes, depending on the hosting network that they plug into. As a consequence, therefore, these devices must consistently reconfigure their routes. As such, MANETs and devices in MANETs lack a central controlling system thus must perform these tasks on their own. As a result of both the literature review and validation of the same, the following research questions were answered;

- The various weaknesses within a MANET ecosystem do contribute to vulnerabilities within the MANET ecosystem.
- These weaknesses of MANET devices and the ecosystem, exposes the devices, data and network to attacks.
- Attacks are experienced within the MANET ecosystem do contribute to loss of confidentiality and availability of the devices and/or data.

References

Adefala., L (2018, March 06). Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries. Fortinet Labs. Retrieved from https://www.fortinet.com/blog/business-and-technology/healthcare-experiences-twice-the-number-of-cyber-attacks-as-othe.html.

Aldaej, A. (2019). Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI). IEEE Access.

Arapi, K. (2018). The Healthcare Industry: Evolving Cyber Threats and Risks (Doctoral dissertation, Utica College).

Chaudhary, A., & Shrimal, G. (2019). Intrusion Detection System Based on Genetic Algorithm for Detection of Distribution Denial of Service Attacks in MANETs. Available at SSRN 3351807.

Das, S., & Pal, S. (2019). Analysis of Energy-Efficient Routing Protocols in Mobile Ad Hoc Network. In Advances in Computer, Communication and Control (pp. 285-295). Springer, Singapore.

Delkesh, T., & Jamali, M. A. J. (2019). EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1897-1914.

Dhindsa, K. S., & Bhushan, B. (2019). Flow-based Attack Detection and Defense Scheme against DDoS Attacks in Cluster based Ad Hoc Networks. International Journal of Advanced Networking and Applications, 10(4), 3905-3910.

Fatima, M., Bandopadhyay, T. K., & Gupta, R. (2019). Unconventional Prediction Algorithm for Quick Route Convergence and Stability in MANET. In Computing, Communication and Signal Processing (pp. 409-418). Springer, Singapore.

Garikipati, V., & Rao, N. N. M. (2019). Secured Cluster-Based Distributed Fault Diagnosis Routing for MANET. In Soft Computing and Signal Processing (pp. 35-51). Springer, Singapore.

Hongach Jr, W. J. (2018). Mitigating Security Flaws in the TCP/IP Protocol Suite (Doctoral dissertation, Utica College).

Inzillo, V., Serianni, A., & Quintana, A. A. (2019). A secure adaptive beamforming mechanism exploiting deafness in direcional beamforming MANET. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII (Vol. 11018, p. 110181F). International Society for Optics and Photonics.

Kamakshi, Y. L., & Kumar, M. M. (2018). A Novel Approach to Secure Route Discovery for Dynamic Source Routing in MANETs.

Kao, D. Y., & Hsiao, S. C. (2018, February). The dynamic analysis of WannaCry ransomware. In Advanced Communication Technology (ICACT), 2018 20th International Conference on (pp. 159-166). IEEE.

Liu, Z., Jin, H., Hu, Y. C., & Bailey, M. (2018). Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control. IEEE/ACM Transactions on Networking, (99), 1-14.

Ngomane, I., Velempini, M., & Dlamini, S. V. (2018). The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks. In 2018 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-5). IEEE.

Rath, M., Swain, J., Pati, B., & Pattanayak, B. K. (2018). Network Security: Attacks and Control in MANET. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 19-37). IGI Global.

Singh, P., Gupta, S., Sejwal, L., & Mohan, A. (2018). Power Issues of MANET. In Information and Communication Technology (pp. 123-128). Springer, Singapore.

Tomar, R. S., Sharma, M. S. P., Jha, S., & Chaurasia, B. K. (2019). Performance Analysis of Hidden Terminal Problem in VANET for Safe Transportation System. In Harmony Search and Nature Inspired Optimization Algorithms (pp. 1199-1208). Springer, Singapore.

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. Computer Law & Security Review, 34(3), 450-466.

Zhang, M., Yang, M., Wu, Q., Zheng, R., & Zhu, J. (2018). Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs. Future Generation Computer Systems, 81, 505-513.

.