Smartphones Hotspots Intrusion Detection System (SHIDS)

Khoula Al Harthy[1], Nazaraf Shah[2], James Shuttleworth[2]
[1]*Computing Department, Middle East College, Oman*
[1]*Coventry University, UK*

Abstract

Ad hoc network is a networking concept, which emerged in the beginning of 1990's. Also known as Peer to Peer (P2P) network, this type of network has facilitated connections among computers. Currently, smartphones are connected to each other wirelessly to share information through hotspot's ad hoc feature. These types of connections have led to many threats and attacks. There have been limited research efforts in threat detection mechanisms for smartphone hotspot connections. This paper proposes a smartphone hotspot Intrusion Detection system (SHIDS) which simulates the detection of the attacks (especially DOS attacks), on smartphone hotspot connections. The proposed architecture is realized into a prototype, which takes into account primary and secondary data collected related to threats and their associated attacks. The novelty of the proposed system is in utilization of historical logs to take decision regarding user access to hotspot connections. In addition the proposed system attempts to reduce the possibility of DoS attack over hotspots connections.

1. Introduction

With the increased usage of client server mode over the network, ad hoc (Peer-to-Peer (P2P)) connections have started to disappear since beginning of 2000. Mobile Ad-Hoc network (MANET) is about mobile devices, which are connected to each other without networking interface node infrastructure is appearing in high usage demand [1]. The last few years have witnessed exponential growth in ad hoc connections, due to increased used of mobile devices especially smartphones. Smartphones have the ability to connect to each other wirelessly to share information. Conti, and Giordano claim that the current network to network infrastructure has changed to phone to phone or person to person paradigm [2]. The smartphone hotspot works over short distances in low transmission rate conditions.

The smartphone ad-hoc connection used for sharing of data faster and less expensive especially with used the internet plan, on the other hand, this new type of ad-hoc means new types of security challenges and threats such as loss of data confidentiality and data privacy [3]. Additionally, the MANET security structure plays an important role in enhancing the MANET experience. Therefore, this paper covers three important aspects: smartphone hotspot security challenges, application of proper data collection methodology and recommendation of best practices to minimize security threats.

2. Related Work

The smartphone hotspot connections work by a technique in which both ends of the ad-hoc network connections are users; one acts as a provider (who share his services with others) and the other end acts as a consumer (who uses the services from the other). This Dynamic mobile ad-hoc Crowd service (DMACS) is an ad-hoc service, which has been adopted to simplify the service process. The DMACS supports the data sharing system such as smartphones sharing the data and files [4]. Hence, the socialization through ad-hoc network has raised one of the important issues of user privacy [5]. Through mobile ad-hoc connections other users over the hotspot network end can expose the users' location. Therefore, mobile ad-hoc can lead to violation of provider privacy. This is called location discolor attack [6]. This type of attack has been considered as an active attack where the attacker tries to find the identity of the other node. Additionally, mobile Ad-Hoc network (MANET) has faced different types of attacks, which affect the security performance as well as data confidentiality. Hence, as the ad-hoc connections have become more and more popular, the MANET attacks have also correspondingly increased. These attacks include session hijacking, Denial of Service attack (DoS), flooding and WEP all of these are leading to or used the Wi-Fi weakness and vulnerabilities [7].

Moreover, the usage of smartphone hotspot application has leads to energy consumption. This act as challenge to security professionals as it difficult to apply security solution for hotspot attacks. Therefore, analytical modules should be used to test the performance and energy consumption used and required during the hotspot services are one [8]. Additionally, the hotspot connection has been

classified as energy consumption services as it cause energy looping and it execute the services it term of loop functionality, which also running multiple background application such as GPS [9]. Some researchers which use to measure the smartphones performance has considered the hotspot with all Wi-Fi access as passive parameters [10]. Over this paper will connect the power consumption with security attacks especially DoS attack as it considered the main approach. Hence, it has been notice that the hotspot it consume the bandwidth more than consuming smartphone hardware components [9], [10].

The paper is organized as follows. In section three we describe smartphones hotspot security issues such as Dos attack, session hijacking and Man in Middle attack. Section four presents research methodology and data analysis. Section five describes proposed Smartphone intrusion detection system (SHIDS)

3.Smartphone hotspot security challenges

Continuous changes in networking paradigm have led to a constant battle of maintaining security in this daynamic environment [2]. The main characteristics of the mobile ad-hoc/hotspots network depend on the user's environment and behavior. Therefore, controlling the ad-hoc environment is considered as a huge challenge, especially considering the lack of effectiveness of detection mechanisms and prevention techniques such as mobile anti malwares. Additionally, traffic monitoring and data ownership is hard to follow. Maintaining the security policy through smartphones are possible but it poses management challenges. These challenges give a rise to malicious attacks and misbehaviors [3] [8]. Moreover, changes in smartphone featuers in each version lead to enhancement in the ad-hoc connections and it also increases the risk and threat levels. That's why they are considered as new generation threats. Thus security techniques and countermeasures are unable to keep pace with mobile ad-hocing connection challenges which lead to failure in data protection and attack preventions.

Moreover the use of smartphones hotspots channel has shown breaches to providers' privacy[8]. The privacy breaches which is highlighted over the hotspots are refered to as breachese of the provider device through detection of the provider location, using GPS, consumption of the internet bytes and access of share folders [11]. Moreover, alongwith user privacy breaches there are other security challenges such as controlling the connection session and managing the users privileges. These challenges have been categorized under weak policy appliance within MANET [12].

Smartphone users are often connected to hotspots these days than to normal modems. The percentage of smart phone access to hotspots is as high as 90% of the phone connections [13]. As mentioned previously, the types of the risks and threats have increased with the increase in the usage of the ad-hocing mechanism. A number of theats have been recognized through number of studies[11][12][13]. The following sub-sections review these threats and risks.

3.1. Malicious node

In a hotspot communication channel an open connection is treated as trust. Therefore, sometimes the provider node seems to be passing the traffic but actually it is a malicious node and it performs a back hole attack by holding all data and traffic from other nodes [14].

3.2. DoS attack

The weak authentication mechanism leads to an increase in the probability of DoS attack. Sstrong Wi-Fi standards such as 802.11 TGi or 802.1X cannot stop DoS attack on wireless hotspot connections [14]. Therefore, it was also noticed that the intrusion detection methods for hotspots are not mature enough to detect the DoS attack or unauthorized access [15].

3.3. Session hijacking

Generally, the connection and the open session between all the nodes through a single hotspot are not encrypted. Therefore, the attacker can eavesdrop on the data and traffic. Additionally, the attacker can use malicious applications which may affect data integrity and confidentiality [16], [17]. The man-in-middle attack is a perfect example of session hijacking. Through the smartphone hotspot connections the attacker enters an open session and steals traffic of that connection [18].

3.4. MiMA: Man in Middle Attack

Man in Middle attack is a traditional way to eavesdrop or steal data from the network connection. In smartphone hotspot the MiMA are demonstrated through a fake hotspot provider who pretend himself as connector or provider to steal data and will be in the middle of the connection as an unauthorized user in the hotspot connections [19]. The MiMA attacker can use multi attack methods such as session hijacking, traffic injection and eavesdropping [20].

4. Research method

This research uses both qualitative and quantitative approaches. The primary data collection method which has been used is a questionnaire which was administered to measure and evaluate the security issue that networks are facing with the increased use of smartphone ad-hoc (hotspot) connections within the domain network.

The survey was distributed to 37 participants from different security and IT professions such as Network Administrators, Security Managers, Cyber Specialists and IT Technicians. These participants have been chosen based on their field experience and security knowledge. Additionally, they were chosen to represent small, medium and large-sized organizations. The interesting revelation of the response was that the concept of Bring Your Own Device (BYOD) is currently well-known in more than 83% of the organizations which allow smartphone connections to their business network.

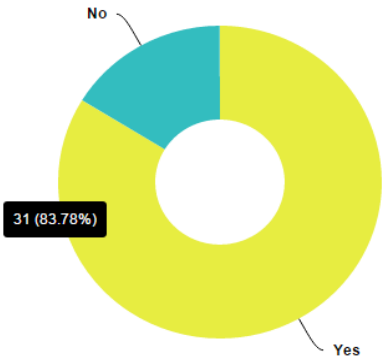


Figure 2. Usage of Smartphones in the Orgnizations

This answer leads to many questions including the capabilities of their network to handle the traffic and its ability to secure both business and personal informations. Therefore, it was necessary to know the Wi-Fi standard currently used in their network to measure and evaluate the performance. 80% of the participants note that 802.11n and 802.11g standards were the most used standards in current networks as shown in the following figure.

Allowing smartphones to connect to company network means allowing hundreds and thousands of unknown devices to consume the bandwidth. Additionally, use the standarded Wi-Fi connections with huge data and traffic load may not be sufficient. Therefore, more than 50% of the participants state that current wireless connections are not performing well with increase in the data size. Therefore, this affects the required performance.

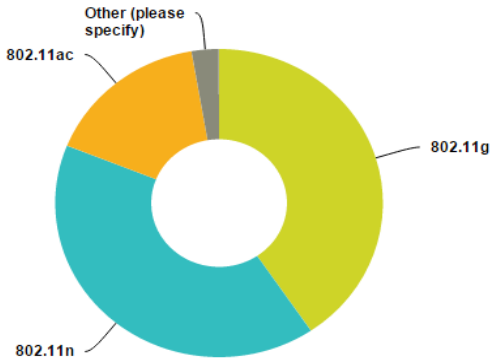


Figure 3. Commonly used Wi-Fi standerd

Moreover, handling the big data transmission over the wireless connections have lead to increased security concerns as well. The smartphones are able to connect to each other and share the internet services through the hotspot point. The participants pointed out that this type of connection has huge security issues, based on different attacks types that have been generated and becomes a root for mobile malwares and backdoor attacks. Therefore, assessing these risks is considered as a challenging task for security managers. However, it was surprising that more than 35% of the participants never checked the impact of allowing smartphones to connect to their network or through personal hotspot. This highlights a serious issue that there are possibilities of security vulnerabilities in their network especially considering the fact that they never update their security methods and control mechanisms.

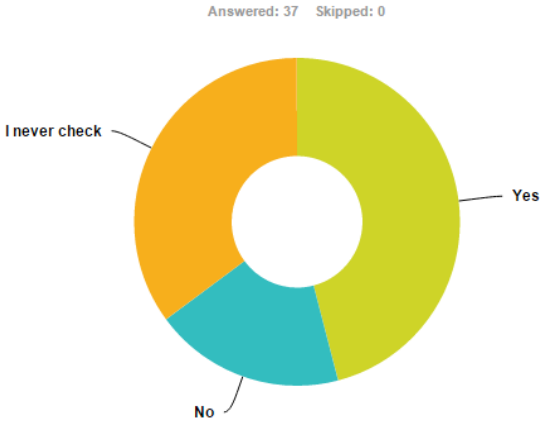


Figure 4. Smartphone hotspot connections are dragging security issues when it connects later to your network

Moreover, the most common challenges of using both hotspot connections and BYOD access over the network have been highlighted by the participants as follows:

Table 1. Challenges of allowing smatphones /hotspots connections over the network

Challenge/Risk	No of participant who highlited/37	Persentage
Bandwidth cunsumption	17	45%
Latency	4	10%
Applications Malwares	13	35%
Policy and control	33	89%
Privacy	20	54%

Within the highlighted challenges and threats, the participants were asked to list the currently used countermeasures which manage the given challenges and risks. Therefore in the following table the most frequently used control and conuntermeasures are listed.

Table 2. Used Countermeasures

Countermeasure	**No of participant who highlited/37**	**Persentage**
Taffic filtering	12	32%
Access List (ACL)	37	100%
IPS/IDS	11	29%
MDM	3	8%
RADUIS SERVER with 802.1x	5	13%

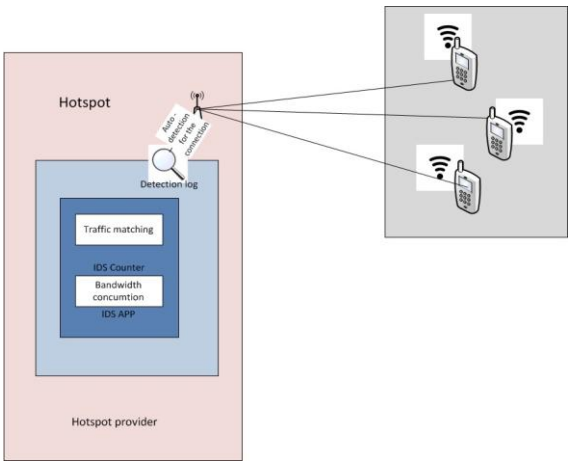
The countermeasures given in Table 2 are sufficient for current security control. However, there are researchers who stated that these control methods face challenges due to increase number of devices and changing technology trends[14][21]. These changes have been reflected into the threats and risk characteristics. The following sections of this paper are the recommend technologies and control methods for the above given challenges with proposed SHIDS architecture. The following parts has been proposed baed in above problems and challenges.

5. Proposed Smartphone Hotspot intrusion detection system (SHIDS)

Intrusion detection system (IDS) is a well known conutermeasure mechanism in standard network security. The IDS works to monitor the internal activity and detect any abnormal events and raise the alarm to the administrator [20]. The current IDS face challenges in monitoring smartphones' functionality and connections. As; smartphones are playing significant roles in exchanging the buiness data today. However, it is considered as uncontrollable connection channels. Therefore, in the light of smartphone hotspot security threats and attacks, this research proposes Smartphone Intrusion Detection System (SHIDS) which is applacible to hotspot connections over the smartphones.

The SHIDS have been classified as solutions which consume the devices' power and reduce users' flexibility [23]. Hence, this research will propose IDS which only functions and acts during the hotspots active connections. The proposed SHIDS works in anomaly detection based on host IDS [24]. The proposed research approach works by comparing the expected traffic to the real traffic and notify if there are any unusual actions [25]. The following present the arhitecture and prototype of the proposed system.

The proposed IDS acts as an app, which runs automatically with the hotspot connections in the smartphones. The IDS contains a counter which works by matching the two important parameters for securing the hotspot connections which are the traffic filtering and the bandwidth consumption as shown in Figure 6. The IDS contains alarm logs which helps in making access decisions for other devices to the hotspot connection.



Figuer 5. Proposed SHIDS framwork

5.1. Traffic count

As mentioned above, the most common attacks through the hotspots are DoS and sniffing attacks. Therefore, the proposed IDS considers traffic filtering and counting of the packets to detect any unusual traffic load. The traffic matching is a component of proposed IDS and contains following features and functionality, which are traffic filtering

and header filtering. The traffic filtering works by matching the normal traffic load which is settled by the users into the real traffic load which is usable. The proposed IDS aims to detect any high traffic load, which can be DoS attacks. Additionally, it detects the specific phone which causes the attack on the IDS employs header filtering to identify the attacker generating high traffic.

5.2. Bandwidth consumption

The bandwidth consumption has been considered as measurement parameter of proposed IDS. Normally the smartphones has low bandwidth range, hence, the bandwidth utilization is considered as a critical issue of the smartphones, that's, because less traffic range should have only small capacity consumption normally the. Therefore, if the traffic matching detects high traffic it reports to bandwidth consumption part which monitors the traffic and disconnects any device generating high traffic.

5.3. Detection log

Maintaining security and avoiding repeated threats are the main concern of any risk management plan. Hence, the proposed IDS will contain detection log, which stores all history alarms. These logs notify the provider (hotspot provider) in future if the detected attacker tries to connect again. Therefore, the IDS contains logs with small memory which store historical logs, saves time of the connection and blocks untrusted connection according to attack source list

5.3.1. Energy consumption. It has been observed that the hotspots connections and attacks also result in energy consumption in smartphones. Therefore, through the proposed system, the energy consumption problem which has been highlighted above will be managed in the following sub-section. This will be done through monitoring the traffic and disconnect the high hotspot usability. Additionally, it will reelect into given alarm through the high consumption statues.

5.4. One time password

As mentioned above DoS is one of the most common attack in mobile hotspot connections. DoS leads to consuming all bandwidth and result into unavailability of services. Therefore, proposing IDS is used for monitoring and detecting hotspot connection. Hence, control of hotspot connection session and to limit the user access are focus of the proposed system SHID. Therefore, One Time Password (OTP) will be proposed as a part of the SHID architecture. OTP is a secure mechanism in which the user should be identified in different codes each time he access to the hotspot connection (Choudhury and Abudin 2014). The propose of apply the OTP is used to reduce the user vulnerabilities in term of accessing time limits. Additionally, the trust OTP will have less effectiveness into smartphones hardware and less power consumption.

OTP have three main methods of authentications which are token based authentication, biometric based authentication and knowledge based authentications (Acharya, Polawar and Pawar 2013). Our proposed approach emplys token base authentication which provide time-limit access to the users. In SHID OTP will be utilized as following steps:

Step 1: the hotspot provider (smartphone who will provide the hotspot connection to the other end) will turn on the hotspot services.

Step 2: The hotspot user will attempts to access in normal hotspot. This involved following actions:

- Check the log and find any history records of requested node. If the answer is yes then the connection will be disabled, otherwise the following step is taken.
- Match the given authentication access to hotspot services, if it matched all authentications requirements then OTP will be generated and send it to other end. The hotspot user will enter the OTP and start the session with limit access.

The utilization of both normal authentication and OTP will considered as two factor authentication to ensure data integrity especially OTP sharing method.

Step 3: the SHID work by filtering the traffic, monitoring the usage and inputs and threats recorded.

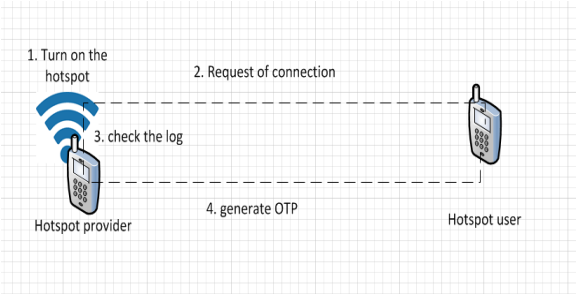


Figure 6. Hotspot OTP generation process in SHID

The proposed structure has been tested in Mobile-OTP application. Mobile-OTP application is free application available in the market and utilized two factors authentications. The functioning of this application required one device to act as server to

receive the login details and check the authentication and then will generate the OTP. The running server side application was required to install java scripts.

The application based on creating profile to the connecting devices (which is similar idea of having the log) as shown in Figure 7.

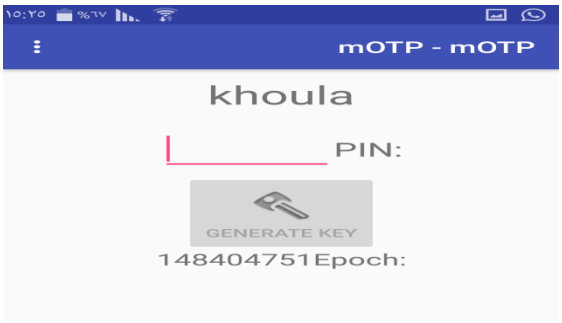
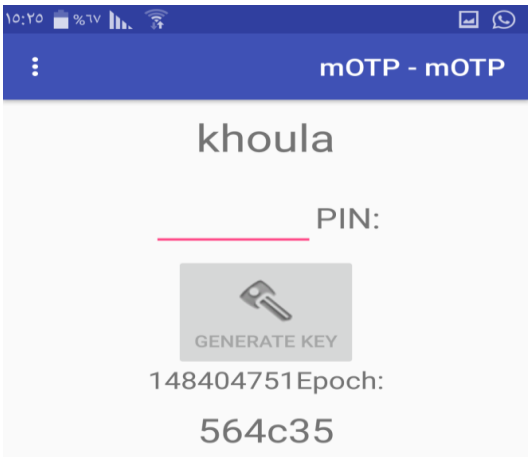


Figure 7. The profile created for the user end

When user identified on the hotspot provider side, the application through his profile will generate the OTP and send it to the user. The OTP will be visible to the provider as shown in the following Figure 8.



Figuer 8. The OPT generated abfter the succfull auethntication

6. Simulation

This section reports on the development of the simulation which utlizes parameters such as number of packets and bandwidth utlizations in hotspot connections.

5.5. Routing and Roaming:

One of the security and management challenges within the smartphones or mobile ad hoc is the routing machnisams. The mobile devices change their locations much faster and roam very often. Therefore, it is hard to apply a policy to these type of connections [19]. Moreover, the ability to detect the attacker over the hotspot connections is considered as a high level secrutiy challenge in current networks. In this paper we simulate this attack The simulation has been implemented in the matlab to demonstrate the DoS attack and sniffing attack over smartphones hotspot connections as shown in Figure 4.

Figure 9 shows simulation of sniffing attack. The packets come from smartphones to access points and within the network the sniffer can intercept the packets and inspect it.

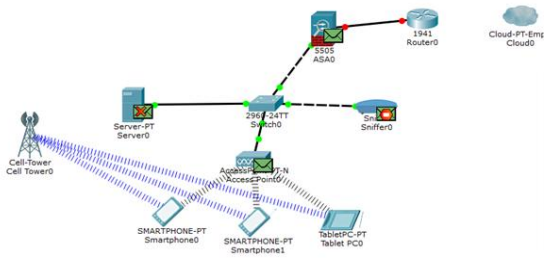


Figure 9. Sniffing attack simulation

The purpose of this simulations is to demonstrate the ability to hack hotspot as shown in Fig 10. The following figure demonstrates the attacker trying to flood other clients by sending large volumes of packets.

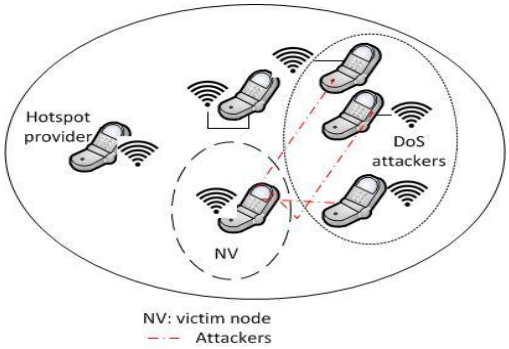


Figure 10. Hotspot DoS attack multi-attackers

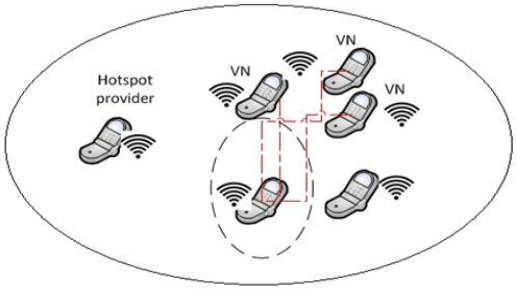


Figure 11. Hotspot DoS attack single attacker

The simulation clearly demonstartes the possibility of hotspot connection attackes through high traffic and bandwidth utlizations. Therefore the proposed IDS will work by tracing back the attack through filtering the traffic and history log. This will help in fast decision making by the smartphones whether to continue enabling the hotspot connection.

Overall, different research efforts have well highlighted these issues [10] and have properly covered the security issues and attacks. These efforts represent the level of importance of this security trend for current network administrators. Hence, it is also observed that currently there are limited solutions available related to mobile hotspot connections [3] [9] [2]. The challenge is to develop effective methods for smartpone hotspot attack prevention, not just only threats detection.

7. Conclusion

This research focuses on smartphone ad-hoc hotspot security issues and challenges. Hence it reports the results of simulating DoS attacks, the most frequent type of attack occurring the hotspots. The proposed SHIDS contains logs that require a small memory to store history logs, it saves time of the connection and it helps to blocks untrusted connections according to the attack source list.

In future, the proposed smartphone hotspot SIDS will be extended to implement ability of detecting comprehensive threats and their countermeasure.

8. References

[1] P. García-López, R.T.a.J.A. (2010) 'Moving routing protocols to the user space in MANET middleware', *Journal of Network and Computer Applications*, vol. 33, no. 5, September , p. 14.

[2] Conti, M. and Giordano, S. (2014) 'Mobile ad hoc networking: milestones, challenges, and new research directions', *Communications Magazine, IEEE,* vol. 52, no. 1, january, p. 12. google.com (2013) *123*, [Online], Available: HYPERLINK "google.com" google.com [5 Nov 2015].

[3] Atallah, È., Bonnefoi, P.F., Burgod, C. and Sauveron, D. (2006) 'Mobile ad hoc network with embedded secure system', seventh edition of e-Smart conference , Nice, France, 5.

[4] Zhang, H., Liu, B., Susanto, H. and Xue, G. (2015) 'Auction-based Incentive Mechanisms for Dynamic Mobile Ad-Hoc Crowd Service', arXiv preprint arXiv:1503.06819, 12.

[5] Chung, E., Joy, J. and Gerla, M. (2015) 'DiscoverFriends: Secure Social Network Communication in Mobile Ad Hoc Networks', *arXiv preprint arXi*, p. 7.

[6] Singh, P., Duhan, M. and Singh, R. (2012) 'An Empirical Analysis On Security And Confidentiality Issues In Mobile Ad-Hoc Networks In Association With Metaheuristic Algorithms', 7.

[7] Joshi, P. (2011) 'Security issues in routing protocols in MANETs at network layer', *Procedia Computer Science*, vol. 3, no. 1877-0509, p. 7.

[8]Chung, Y.W. (2012) 'Performance Analysis of Energy Consumption of Smartphone Running Mobile Hotspot Application', *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, Sep, p. 6..

[9] Banerjee, A., Chong, L.K., Chattopadhyay, S. and Roychoudhury, A. (2014) 'Detecting energy bugs and hotspots in mobile apps', 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering, 11.

[10] Ra, M.R., Paek, J., Sharma, A.B., Govindan, R., Krieger, M.H. and Neely, M. (2010) 'Energy-Delay Tradeoffs in Smartphone Application', 8th international conference on Mobile systems, applications, and services, ACM, 15.

[11] Chung, Y.W. (2013) 'Performance Analysis of Energy Consumption of Smartphone Running Mobile Hotspot Application.', *International Journal of Smart Grid and Clean Energy*, Jan, p. 6.

[12] Abogharaf, A., Palit, R., Naik, K. and Singh, A. (2012) 'A methodology for energy performance testing of smartphone applications', 7th International Workshop on automation of Software Test (AST), 2012 , 6.

[13] Afanasyev, M., Chen, T., Voelker, G.M. and Snoeren, A.C. (2008) 'Analysis of a mixed-use urban wifi network: when metropolitan becomes neapolitan.', 8th ACM SIGCOMM conference on Internet measurement, ACM, 13.

[14] Manikandan, S.P. and Manimegalai, R. (2012) 'Survey on mobile Ad Hoc network attacks and mitigation using routing protocols', *American Journal of Applied Sciences*, vol. 9, no. 11, Sep, p. 7.

[15] Balachandran, A., Voelker, G.M. and Bahl, P. (2005) 'Wireless hotspots: current challenges and future directions', *Mobile Networks and Applications,* vol. 10, no. 3, p. 9.

[16] Leavitt, N. (2011) 'Mobile security: finally a serious problem', *IEEE computer trancsuction*, vol. 44, no. 6, June, p. 14.

[17] Bharti, A.K., Goyal, M. and Chaudhary, M. (2013) 'A Review on Detection of Session Hijacking and Ip Spoofing', *International Journal of Advanced Research in Computer Science,* vol. 4, no. 9, July.

[18] Harper, E. (2014) How to Protect Your Privacy on Public WiFi Networks, 29 Oct, [Online], Available: at http://www.techlicious.com/tip/how-to-protect-your-privacy-on-public-wifi-networks/ [6 Nov 2015].

[19] Matos, A., Romao, D. and Trezentos, P. (2012) 'Secure hotspot authentication through a Near Field Communication side-channel.', Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference , 8.

[20] Noor, M.M. and Hassan, W.H. (2013) 'Wireless networks: developments, threats and countermeasures.', International Journal of Digital Information and Wireless Communications (IJDIWC), , vol. 3, no. 1, p. 17.

[21] Ning, W., Wang, H. and Wang, W. (2014) 'Security issues on mobile ad hoc network for mobile commerce.', In Proceedings of Informing Science & IT Education Conference., 11.

[22] Shakshuki, E.M., Kang, N. and Sheltami, T.R. (2013) 'EAACK - A Secure Intrusion-Detection System for MANETs', IEEE Transactions On Industrial Electronics, vol. 60, no. 3, March, p. 10

[23] Halilovic, M. and Subasi, A. (2012) 'Intrusion Detection on Smartphones', arXiv preprint arXiv:1211.6610., 28 Nov, p. 6.

[24] Burguera, I., Zurutuza, U. and Nadjm-Tehrani, S. (2011) 'Crowdroid: behavior-based malware detection system for android.', n Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, ACM., 11.

[25] Polla, M.L., Martinelli, F. and Sgandurra, D. (2013) 'A Survey on Security for Mobile Devices', IEEE Communications Surveys & Tutorials, vol. 15, no. 1, First Quarter, p. 26

