A Study on Various Attacks and Solutions in Smart Phone Ad Hoc Networks (SPANs)

Mr.M.Krishnamoorthi[1], Mr.A.Venugopal[2]
[1, 2] Dept of Computer Science
[1, 2] K.S.Rangasamy College of Arts and Science College (Autonomous), Tiruchengode, Tamilnadu, India

Abstract- *Smart phone ad hoc or Smartphone ad hoc networks (SPANs) evolve from the underlying concept, architecture and technology behind a wireless ad hoc network. It is blended with ad hoc networking technology. A Smartphone can establish ad hoc networks among other mobile phone devices. SPANs (smart phones ad hoc network) use the mechanism behind Wi-Fi ad-hoc mode, which allows phones to share confidential information directly among each other, through a transparent neighbour and route discovery mechanism. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop routing (ad hoc routing) and relays and there is no notion of a group leader, so everyone can involve and leave at will without destroying the network. And Security can be achieved by encrypting and decrypting the data and make them unable to read that from the malicious users. In this paper we discuss about SPANs and its applications and various attacks and its solutions which exist in the ad hoc network. Various attacks are performed in this network such as attacks performed in hardware and software, password cracking and etc.. The wirelessly network always required security in the form of data integrity, confidentiality, authenticity and etc.*

Keywords- Ad hoc Network, Routing, SPANs, Security, Cryptography

I. INTRODUCTION

These days, trendy of Smartphones are rapidly getting popularity. The powerful superior processing and wireless networking capabilities of these enable users to communicate and share confidential information easily than exist. In forming smart phone ad hoc networks (SPANs) from one part of mobile ad hoc network (MANET) can connect to each other wirelessly without existing network architecture.

This feature is extending the usage of and also makes information sharing more convenient at lowest cost and less time. In particular concern is the security of personal and business information now stored on Smartphones. More and more users and businesses use Smartphones to communicate, but also to plan and organize their users' work and also private life. Indeed, Smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user. All (smart phone ad hoc networks (SPANs) and Mobile ad hoc networks (MANETs), are preferred targets of attacks. These attacks exploit weaknesses inherent in Smartphones that can come from the communication mode like Short Message Service (SMS, text messaging), Multimedia Messaging Service (MMS), wifi, Bluetooth and GSM, and etc. There are also exploits that target software vulnerabilities in the browser or operating system.

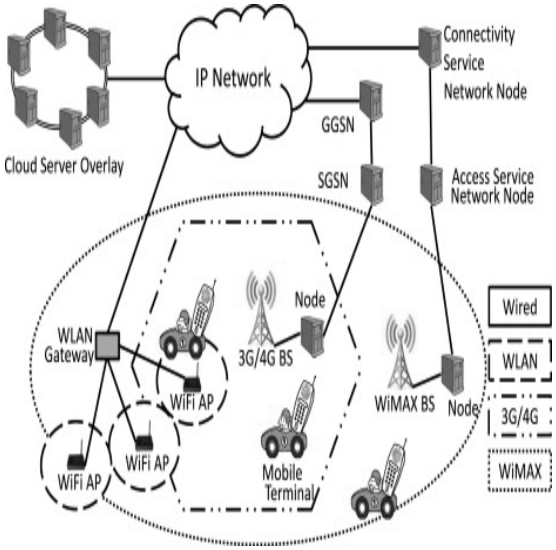

Fig 1. Smart phone ad hoc network(SPANs)

And some malicious software relies on the weak knowledge of an average user. Security countermeasures are being developed and applied to Smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

II. LITERATURE REVIEW

Smartphones has become a very popular word and rapidly increasing part in today's networking area to share information to each other. An incredible growth has appeared

in the development of mobile devices such as, Smartphone, PDA, and laptops with a variety of mobile computing, networking and security technologies. In addition, with the development of wireless technology and internet it becomes much easier and not limited by the particular office or home or organizations. Thus, more and more people have accepted those mobile devices and gives support to rise in the technology of mobile AdHoc networks(MANET).Smartphones AdHoc network(SPANs) is described as a form of human-computer interaction by which a computer is expected to be transported during normal usage. Smartphone ad hoc Network (SPANs) can be said as the collection of three major concepts: hardware, software and communication. The concepts of hardware are dependendent on Smartphone devices, such as Smartphone and laptop, or their mobile components. The second concept of Software in Smartphone AdHoc Network (SPANs) is the numerous mobile applications in the particular hardware devices, such as the mobile browser, anti-virus software and games stored at remote distance on some other servers. Finally, the communication issue includes the infrastructure of Smartphone AdHoc Networks(SPANs), protocols and data delivery in their use, which must be transparent to end users. With the use of the cloud-computing concept, it is easier to develop mobile computation somewhat easier.

III. SECURITY DIFFICULTIES AND CHALLENGES

A. Security

Security design must consider principles of time and location whereas Smartphone ad hoc Networks(SPANs) is increased in multiple- environment openly. Eavesdropping of communication media, Denial Of Service (DOS) and modification of information are patterns of attacks performed by a hacker due to obtaining control of user instruments. Moving across various networks smoothly without user-aware of what network is passing forms main objective to carry out reliable services without more insist on infrastructure. Protection from unauthorized user (security), prevention of access by an attacker through unauthorized techniques (integrity), providing accessibility for user entirely (availability) and avoiding an entity from refusing former actions (non-repudiation) are important factors in the security model. Noticing type of transferring data, possible distortion or misuse, weaknesses and features, the security issues in mobile ad hoc network(MANET) infrastructure environments can be illustrated.

- ✓ Lack of authentication
- ✓ Recent flaws due to former attacks
- ✓ Unplanned growth to improve
- ✓ Lack of suitable security solution
- ✓ Weak control
- ✓ Elements interaction issues regarding upgrades
- ✓ Weak application

Although technical capability in the side of users maybe relies on distributed security mechanism, some circumstances require more security to address and ubiquitous computing enlist security in different approaches Particular security requirements and solutions can be determined as below:

Interoperability: Every domain in Smartphone Ad hoc Network(SPANs)environment is addressed by its proper security solution so it needs to be matching with existing local security solution.

Availability: Whereas the environment is dynamic, incoming and outgoing entries affect networks entirely, so proper operation named Ubiquitous Device Management (UDM) act against alteration of environment to maintain availability.

Protection: Credential in environment can be existed at different layers using IP Security (IPSec) and Secure Socket Layer (SSL). Different security protocols exist in different network infrastructure and unified protocols are required at the ubiquitous network level.

Delegation: A running service regarding different networks and their mobile parts can change the network so it is necessary for users to authorize alterations and delegate their right to a management function running on their behalf.

Platform safety: this networks are enhanced with capability to download application securely that allow proportional update or reconfigure. If there is no limitation on downloadable source for application so malicious applications may penetrate and reconfigure an instrument. For this reason, it is urgent to protect the platform from this kind of attacks.

Single sign on (SSO): Whereas, users often need to access multiple service providers getting involved with multiple authentications and various devices, services and networks, so it is required to implement a single sign-on solution which reforms the initiation for entries to authenticate once in all network domains to include reliable leaving and joining of Smartphone ad hoc networks(SPANs)without disturbances.

Content safety: While significant capability of delivering multiple services by Smartphone ad hoc networks (SPANs) to users is noticed, assurance of being secure for providers in digital environment is guaranteed using a Digital Right Management (DRM) system to implement in ubiquitous instruments.

B. Challenges

The further aspects and the extended functionality that Smartphone AdHoc networks(SPANs) offers make it inclined to more vulnerabilities and disclosures concluding an extra responsibility to the security subsystem.

The extended computing boundary: The new computing environment indicates the intangible conventional computing with related constraints of user locations. On this environment traditional methods concentrating solely on digital security are insufficient.

Privacy issues: Because of physical outreach of Smartphone AdHoc networks(SPANs),privacy of users is become as perverse task. More intelligent spaces and computing capabilities that are openly extensive supplied by natural construction. These spaces can be captured and utilize context information. So the system forms a distributed observation system that can capture too much information about users and donates confidence of track prevention for users.

Trust security: Trust is an association between two entities such that one entity credits other trusted entity and also is a representation of being reliable, secure and trustworthy in any interaction with the node. A trust security task will supply implements qualifying to utilize and doing performance of security related decisions autonomously.

Social issues: Social cues can be extremely important for building models of security, privacy, and trust in a system. Knowing what other people think, talking with other people affected by the system (or responsible of it), and the general social pressures of belonging to a group can all affect people's perceptions of technology Individual, group and behaviours are categorized as social issues. New ways of communicate, technologies, interaction and also human behaviour is considered.

User interaction issues: Because of the nature of group interactions between users in the space, it is not easily possible to deny seeing or hearing of user information, thus consideration to overcome due to this issue must be taken into security plan by jointing physical and virtual aspects of access control with each other. Information operation: It is a serious concern in the network in the networks that is over new types of threats. It can be defined as actions taken that affect adversary information and information systems while defecting one's own information and information systems. In this way cyber terrorists and other techno-villains can exploit computer networks, inject misleading information, steal electronic assets or disrupt critical services monitor to prevent.

Security policies: Implying a flexible and convenient approach to define and manage security policies in a dynamic context-aware form is dominant for ubiquitous computing. Policy Management tools provide administrators the capability to specify, implements, and imposes rules to exercise greater control over the behaviour of entities in their systems. The policy management software maintains an exhaustive database of corresponding device and resource interfaces. With the increase of heterogeneous device-specific and vendor-specific interfaces, these tools may need to be updated frequently to accommodate new hardware or software, and the system normally becomes difficult to manage. As a result, general purpose low-level management tools are limited in their functionality, and are forced to implement only generic or coarse-grained policies.

IV. ATTACKS IN SPANs

There are many attacks are involved in Smartphone ad hic network to steal confidential data those attacks are listed below:

A. Attacks based in Communication

Attacks in SMS and MMS: Some Smartphone models have problems in managing binary SMS messages. It is possible, by sending an ill-formed block, to cause the phone to restart, leading to the denial of service attacks. If a user with a received a text message containing a Chinese character, it would lead to a denial of service. In another case, while the standard requires that the maximum size of a Nokia Mail address is 32 characters, some Nokia phones did not verify this standard, so if a user enters an email address over 32 characters, that leads to complete dysfunction of the e-mail handler and puts it out of commission. This attack is called "curse of silence". A study on the safety of the SMS infrastructure revealed that SMS messages sent from the Internet can be used to perform a distributed denial of service (DDoS) attack against the Smartphone (SPANs) infrastructure of a big city. The attack exploits the delays in the delivery of messages to overload the network.

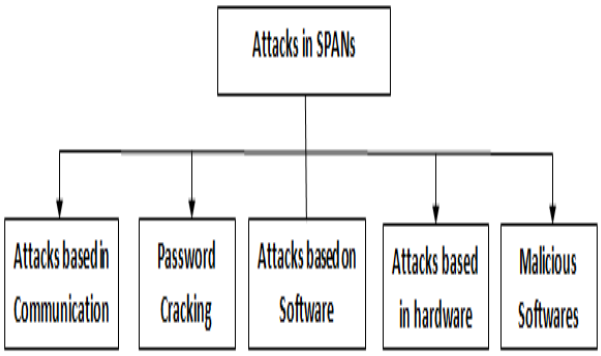

Fig 2.Attacks in SPANs

B.Password Cracking

Attacks based on the GSM networks*:* The attacker may try to break the encryption of the Smartphone network. The GSM network encryption algorithms belong to the family of algorithms called A5. Due to the policy of security through obscurity it has not been possible to openly test the robustness of these algorithms. There were originally two variants of the algorithm: A5/1 and A5/2 (stream ciphers), where the former was designed to be relatively strong, and the latter was designed to be weak on purpose to allow easy cryptanalysis and eavesdropping. ETSI forced some countries (typically outside Europe) to use A5/2. Since the encryption algorithm was made public, it was proved it was possible to break the encryption: A5/2 could be broken on the fly, and A5/1 in about 6 hours .In the 3GPP approved a change request to prohibit the implementation of A5/2 in any new Smartphones, which means that it has been decommissioned and is no longer implemented in mobile phones.

Stronger public algorithms have been added to the GSM standard, the A5/3 and A5/4 (Block ciphers), otherwise known as KASUMI or UEA1 published by the ETSI. If the network does not support A5/1, or any other A5 algorithm implemented by the Smartphone, then the base station can specify A5/0 which is the null-algorithm, whereby the radio traffic is sent unencrypted. Even in case mobile phones are able to use 3G or 4G which have much stronger encryption than 2G GSM, the base station can downgrade the radio communication to 2G GSM and specify A5/0 (no encryption) .This is the basis for eavesdropping attacks on mobile radio networks using a fake base station commonly called an IMSI catcher.

Attacks based on Wi-Fi: An attacker can try to eavesdrop on Wi-Fi communications to derive information. This type of attack is not unique to Smartphones, but they are very vulnerable to these attacks because very often the Wi-Fi is the only means of communication they have to access the internet. The security of wireless networks (WLAN) is thus an important subject. Initially, wireless networks were secured by WEP keys. The weakness of WEP is a short encryption key which is the same for all connected clients. In addition, several reductions in the search space of the keys have been found by researchers. Now, most wireless networks are protected by the WPA security protocol. WPA is based on the "Temporal Key Integrity Protocol (TKIP)" which was designed to allow migration from WEP to WPA on the equipment already deployed. The major improvements in security are the dynamic encryption keys. For small networks, the WPA is a "pre-shared key" which is based on a shared key. Encryption can be vulnerable if the length of the shared key is short. With limited opportunities for input mobile phone users might define short encryption keys that contain only numbers. This increases the likelihood that an attacker succeeds with a brute-force attack.

The successor to WPA, called WPA2, is supposed to be safe enough to withstand a brute force attack. As with GSM, if the attacker succeeds in breaking the identification key, it will be possible to attack not only the phone but also the entire network it is connected to many Smartphones for wireless LANs remember they are already connected, and this mechanism prevents the user from having to re-identify with each connection. However, an attacker could create a WIFI access point twin with the same parameters and characteristics as the real network. Using the fact that some Smartphones remember the networks, they could confuse the two networks and connect to the network of the attacker who can intercept data if it does not transmit its data in encrypted form.

C. Attacks based on software

Web Browser: The mobile web browser is an emerging attack vector for mobile devices. Just as common Web browsers, mobile web browsers are extended from pure web navigation with widgets and plug-ins, or are completely native mobile browsers In this case, there was a vulnerability based on a stack-based buffer overflow in a library used by the web browser. Vulnerability in the web browser for Android was discovered in October 2017.As the iPhone vulnerability above, it was due to an obsolete and vulnerable library. A significant difference with the iPhone vulnerability was Android's sandboxing architecture which limited the effects of this vulnerability to the Web browser process.

Operating System: Sometimes it is possible to overcome the security safeguards by modifying the operating system itself. As real-world examples, this section covers the manipulation of firmware and malicious signature certificates. These attacks

are difficult. In 2017, vulnerabilities in virtual machines running on certain devices were revealed. It was possible to bypass the byte code verifier and access the native underlying operating system. The results of this research were not published in detail. The firmware security of Nokia's Symbian Platform Security Architecture (PSA) is based on a central configuration file called SWI Policy. In 2017 it was possible to manipulate the Nokia firmware before it is installed, and in fact in some downloadable versions of it, this file was human readable, so it was possible to modify and change the image of the firmware. This vulnerability has been solved by an update from Nokia In theory Smartphones have an advantage over hard drives since the OS files are in ROM, and cannot be changed by malware. However, in some systems it was possible to circumvent this: in the Symbian OS it was possible to overwrite a file with a file of the same name. On the Windows OS, it was possible to change a pointer from a general configuration file to an editable file.

D. Attacks based on Hardware

Juice Jacking: Juice Jacking is a physical or hardware vulnerability specific to mobile platforms. Utilizing the dual purpose of the USB charge port, many devices have been susceptible to having data infiltrated from, or malware installed onto a mobile device by utilizing malicious charging kiosks set up in public places or hidden in normal charge adapters.

Jail braking and Rooting: Jail-breaking is also a physical access vulnerability, in which mobile device users initiate to hack into the devices to unlock it, and exploit weaknesses in the operating system. Mobile device users take control of their own device by jail-breaking it, and customize the interface by installing applications, change system settings that are not allowed on the devices. Thus, allowing tweaking the mobile devices operating systems processes, run programs in the background, thus devices are being exposed to variety of malicious attack that can lead to compromise important private data.

E. Malicious Software

As Smartphones are a permanent point of access to the internet, they can be compromised as easily as computers with malware. A malware is a computer program that aims to harm the system in which it resides. Trojans, worms and viruses are all considered malware.

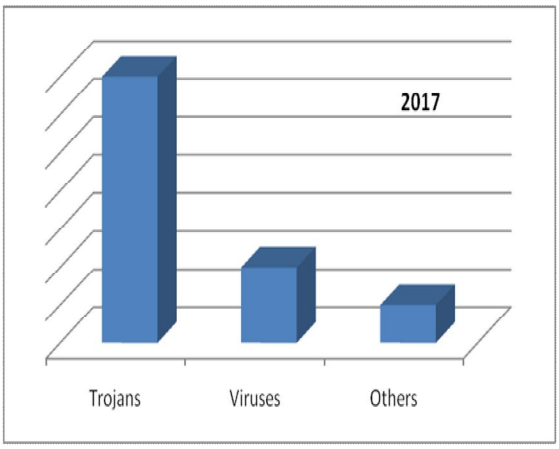

Fig 3.Malwares statistics in year 2017

A Trojan is a program that is on the Smartphone and allows external users to connect discreetly. A worm is a program that reproduces on multiple computers across a network. A virus is malicious software designed to spread to other computers by inserting itself into legitimate programs and running programs in parallel. However, it must be said that the malware are far less numerous and important to Smartphones as they are to computers. Example of malicious software is Ransom ware, spyware and Trojan etc.

V.SOLUTIONS FOR SPANs ATTACKS

The security mechanisms in place to counter the threats in Various Types of Smartphone Attacks. Here Some Solutions are listed below for Smartphone Ad hoc Networks (SPANs).

A.Security in Smartphone OS

The first layer of security in a smartphone is the operating system (OS). Beyond needing to handle the usual roles of an operating system scheduling processes on the device, it must also establish the protocols for introducing external applications and data without introducing risk.

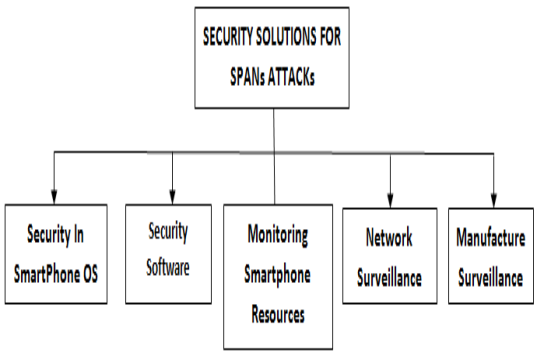

Fig 5.SPANs Attacks Solutions

A central paradigm in mobile operating systems is the idea of a sandbox. Since smartphones are currently designed to accommodate many applications, they must have mechanisms to ensure these applications are safe for the phone itself, for other applications and data on the system, and for the user. If a malicious program reaches a mobile device, the vulnerable area presented by the system must be as small as possible. Sandboxing extends this idea to compartmentalize different processes, preventing them from interacting and damaging each other. Based on the history of operating systems, sandboxing has different implementations. The following points highlight mechanisms implemented in operating systems, especially Android.

Rootkit Detectors:the intrusion of a rootkit in the system is a great danger in the same way as on a computer. It is important to prevent such intrusions, and to be able to detect them as often as possible. Indeed, there is concern that with this type of malicious program, the result could be a partial or complete bypass of the device security, and the acquisition of administrator rights by the attacker. If this happens, then nothing prevents the attacker from studying or disabling the safety features that were circumvented, deploying the applications they want, or disseminating a method of intrusion by a rootkit to a wider audience. We can cite, as a defense mechanism, the Chain of trust in iOS. This mechanism relies on the signature of the different applications required to start the operating system, and a certificate signed by Apple. In the event that the signature checks are inconclusive, the device detects this and stops the boot-up.If the Operating System is compromised due to Jail breaking, root kit detection may not work if it is disabled by the Jailbreak method or software is loaded after Jailbreak disables Rootkit Detection.

Process Isolation: Android uses mechanisms of user process isolation inherited from Linux. Each application has a user associated with it, and a tuple (UID, GID). This approach serves as a sandbox: while applications can be malicious, they can not get out of the sandbox reserved for them by their identifiers, and thus cannot interfere with the proper functioning of the system. For example, since it is impossible for a process to end the process of another user, an application can thus not stop the execution of another.

File Permissions: From the legacy of Linux, there are also file system permissions mechanisms. They help with sandboxing: a process cannot edit any files it wants. It is therefore not possible to freely corrupt files necessary for the operation of another application or system. Furthermore, in Android there is the method of locking memory permissions. It is not possible to change the permissions of files installed on the SD card from the phone, and consequently it is impossible to install applications.

Memory Protections: In the same way as on a computer, memory protection prevents privilege escalation. Indeed, if a process managed to reach the area allocated to other processes, it could write in the memory of a process with rights superior to their own, with root in the worst case, and perform actions which are beyond its permissions on the system. It would suffice to insert function calls are authorized by the privileges of the malicious application.

B.Security Software

Above the operating system security, there is a layer of security software. This layer is composed of individual components to strengthen various vulnerabilities.prevent malware, intrusions, the identification of a user as a human, and user authentication. It contains software components that have learned from their experience with Smartphone security. however, on smartphones, this software must deal with greater constraints.

Antivirus and Firewall: An antivirus software can be deployed on a device to verify that it is not infected by a known threat, usually by signature detection software that detects malicious executable files. A firewall, meanwhile, can watch over the existing traffic on the network and ensure that a malicious application does not seek to communicate through it. It may equally verify that an installed application does not seek to establish suspicious communication, which may prevent an intrusion attempt

Visual Notifications: In order to make the user aware of any abnormal actions, such as a call they did not initiate, one can link some functions to a visual notification that is impossible to circumvent. For example, when a call is triggered, the called number should always be displayed. Thus, if a call is triggered by a malicious application, the user can see, and take appropriate action.

Turing Test: In the same vein as above, it is important to confirm certain actions by a user decision. The Turing test is used to distinguish between a human and a virtual user, and it often comes as a captcha.

Biometric Identification: Another method to use is biometrics. Biometrics is a technique of identifying a person by means of their morphology or their behavior. One advantage of using biometric security is that users can avoid having to remember a password or other secret combination to authenticate and prevent malicious users from accessing their

device. In a system with strong biometric security, only the primary user can access the smartphone.

C.Monitoring SmartPhone Resources

When an application passes the various security barriers, it can take the actions for which it was designed. When such actions are triggered, the activity of a malicious application can be sometimes detected if one monitors the various resources used on the phone. Depending on the goals of the malware, the consequences of infection are not always the same; all malicious applications are not intended to harm the devices on which they are deployed. The following sections describe different ways to detect suspicious activity.

Battery: Some malware is aimed at exhausting the energy resources of the phone. Monitoring the energy consumption of the phone can be a way to detect certain malware applications.

Memory Usage: Memory usage is inherent in any application. However, if one finds that a substantial proportion of memory is used by an application, it may be flagged as suspicious.

Network Traffic: On a smartphone, many applications are bound to connect via the network, as part of their normal operation. However, an application using a lot of bandwidth can be strongly suspected of attempting to communicate a lot of information, and disseminate data to many other devices. This observation only allows a suspicion, because some legitimate applications can be very resource-intensive in terms of network communications, the best example being streaming video.

Services: One can monitor the activity of various services of a smartphone. During certain moments, some services should not be active, and if one is detected, the application should be suspected. For example, the sending of an SMS when the user is filming video: this communication does not make sense and is suspicious; malware may attempt to send SMS while its activity is masked.

D.Network Surveillance

Network traffic exchanged by phones can be monitored. One can place safeguards in network routing points in order to detect abnormal behavior. As the mobile's use of network protocols is much more constrained than that of a computer, expected network data streams can be predicted (e.g. the protocol for sending an SMS), which permits detection of anomalies in mobile networks.

Spam Filters: As is the case with email exchanges, we can detect a spam campaign through means of mobile communications (SMS, MMS). It is therefore possible to detect and minimize this kind of attempt by filters deployed on network infrastructure that is relaying these messages.

Encrypt Informations: Because it is always possible that data exchanged can be intercepted, communications, or even information storage, can rely on encryption to prevent a malicious entity from using any data obtained during communications. However, this poses the problem of key exchange for encryption algorithms, which requires a secure channel.

E.Manufacturer Surveillance

In the production and distribution chain for Smartphone devices, it is the responsibility of manufacturers to ensure that devices are delivered in a basic configuration without vulnerabilities. Most users are not experts and many of them are not aware of the existence of security vulnerabilities, so the device configuration as provided by manufacturers will be retained by many users.

Remove Debug Mode: Phones are sometimes set in a debug mode during manufacturing, but this mode must be disabled before the phone is sold. This mode allows access to different features, not intended for routine use by a user. Due to the speed of development and production, distractions occur and some devices are sold in debug mode. This kind of deployment exposes mobile devices to exploits that utilize this oversight.

Default Setting: When a smartphone is sold, its default settings must be correct, and not leave security gaps. The default configuration is not always changed, so a good initial setup is essential for users. There are, for example, default configurations that are vulnerable to denial of service attacks.

Audit Apps: Along with smart phones, appstores have emerged. A user finds themselves facing a huge range of applications. This is especially true for providers who manage appstores because they are tasked with examining the apps provided, from different points of view (e.g. security, content). The security audit should be particularly cautious, because if a fault is not detected, the application can spread very quickly within a few days, and infect a significant number of devices.

Detect Suspicious Apps: When installing applications, it is good to warn the user against sets of permissions that, grouped together, seem potentially dangerous, or at least suspicious.

Frameworks like such as Kirin, on Android, attempt to detect and prohibit certain sets of permissions.

Revocation Procedures: Along with app stores appeared a new feature for mobile apps: remote revocation. First developed by Android, this procedure can remotely and globally uninstall an application, on any device that has it. This means the spread of a malicious application that managed to evade security checks can be immediately stopped when the threat is discovered.

Avoid Heavily Customized Systems: Manufacturers are tempted to overlay custom layers on existing operating systems, with the dual purpose of offering customized options and disabling or charging for certain features. This has the dual effect of risking the introduction of new bugs in the system, coupled with an incentive for users to modify the systems to circumvent the manufacturer's restrictions. These systems are rarely as stable and reliable as the original, and may suffer from phishing attempts or other exploits.

VI.SECURITY REQUIREMENT IN SPANs

A SPANs is a special form of network. It shares few commonalities with a usual Each network, but also exhibitions many features that are sole to it. The services of security must be protecting the info communicated over the n/w and the resources from attacks and nodal misconduct in a SPANs. The vital security necessities are listed below in SPANs:

A. Data confidentiality

The security mechanism needs to make sure that no message in the n/w is understood with the aid of anybody besides supposed recipient. In aSPANs, the problematic of confidentiality ought to address the next necessities.

B. Availability

This necessities make sure which the SPANS services should be accessible always even in occurrence of an external or internal attacks e.g. DoS. Dissimilar methods have been defined thru investigators to accomplish this objective. While some mechanisms create exploit of additional communiqué among nodes, others propose utilize of a central access control system to make sure successful transfer of all message to its receiver.

C. Data freshness

It implies which the info is current and make sure which no adversary can replay old messages. This necessity is especially significant when the SPANs Smartphone exploit shared keys for message communiqué, where a potential adversary can launch a replay attack exploiting the old key as the newest key is being propagated to each the nodes in the SPANs.A time-precise counter may be insert to all packet to check the cleanness of the packet.

D. Self-organization

Every node in a SPANS must be self-organizing and self-recuperation. This characteristic of a SPANS additionally poses good challenges to safety. The SPANS dynamic nature makes it occasionally not possible to installation any pre-installed hared key mechanism the several nodes and the BS. A no.of key pre-distribution systems have been define inside the context of symmetric encryption However, for software of public-key cryptographic techniques an efficient mechanism for key distribution could be very a great deal crucial. It's perfect that the nodes in a SPANs self-establish among themselves no longer simplest for multi-hop routing however also to carryout key control and growing trust relations.

E. Secure localization

In many conditions, it will become essential to accurately and automatically discover each Smartphone node in a SPANs. SPANs planned to locate errors would precise localities of Smartphone nodes recognizing the faults. A capacity adversary can without difficulty provide and manipulate fake locality info with the aid of reporting fake sign asset, replaying messages and so on. If the info statistics isn't always secured properly. The writers in have defined a way called as verifiable multilateration (VM). In multilateration, the position of a device is accurately computed from a sequence of known reference points. The authors have utilized distance bounding and authenticate ranging to make sure accurate place of a node. Due to the distance bounding usage, an attacking node can best successful its claimed distance from a situation factor. However, to make certain region consistency, the attacker would additionally need to show that its distance from every other reference factor is shorter. As it isn't always viable for the attacker to prove this, it's miles viable to come across the attacker. The system is a decentralized range self-governing localization scheme. It's supposed that the locators are trusted and can't be compromised thru any attacker. Exploiting the info from each the beacons which a Smartphone node accepts, it calculates it estimated locality depend on the locators coordinates. The Smartphone node then calculates

overlapping antennas are exploiting a majority election scheme. The last Smartphone node locality is determined through computing the gravity center of the overlapping antenna area.

F. Time synchronization

The applications in Smartphone necessitate time synchronization. Any security mechanism must additionally be time synchronized. A collaborative SPANS can also necessitate synchronization among a gathering of Smartphones. In define a gathering of secure synchronization protocols for multi-hop sender receiver and group synchronization.

G. Authentication

The communicating node is the one that it claims to be. An adversary can't only alteration data packets but also can modify a packet stream thru inserting fabricated packets. It's, therefore, vital for a receiver to have a mechanism to confirm which the received packets have indeed arrive from the actual sender node.

VII. CONCLUSION

SPANs have received a Superior attention in now days. These networks are mainly used for improving efficiency and safety of the transportation between the SPAN nodes. As we know that wireless medium is used in SPAN for transmission of data or information from one to another so there are chances of various attacks in SPANs. This paper includes various attacks in SPANs. It also includes various properties of attacker, what are the security requirements which are required for the safety of the SPANs. As we know that users' want safety and security on the future and it may be possible by implementing secure and safe SPAN network for users.

REFERENCES

[1] Dwarapu Suneetha, Mogalla Shashi," Research Issues and Developments in Social Network Analytics" International Journal of Computer Science and Network, Volume 6, Issue 6, December 2017.

[2] Amosa Babalola,Onyeka Ndidi, Olaniyi Busayo,Babafemi Olusola" Mobile Agent for Monitoring and Evaluation of Security Applications in a Network Environment" International Journal of Computer Science and Network, Volume 6, Issue 6, December 2017.

[3] Sandeep patil, dr. L.s. Admuthe, dr. M. R. Patil"A Review on Trust Based Secure Routing Protocols in Ad-hoc Networks" International Journal of Advanced Research in Computer Science.

[4] Husna Jamal Abdul Nasir, Ku Ruhana Ku-Mahamud, Eiji Kamioka" Enhanced Ant-based Routing For Improving Performance of Wireless Sensor Network" International Journal of Communication Networks and Information Security vol. 9, no. 3, December 2017.

[5] Jhum Swain, Binod Kumar Pattanayak, Bibudhendu Patimilu" A New Approach for DDoS Attacks to Discriminate The Attack Level and Provide Security for DDos Nodes in MANET" International Journal of Communication Networks and Information Security vol. 9, December 2017.

[6] S. Thirumurugan, Jasmine Beulah Gnanadurai" A Novel Application based Generic Cluster Creation Mechanism in Ad Hoc Networks" International Journal of Computer Networks and Applications, vol. 4, December 2017.