Vol 2 Issue 9 March 2013

Impact Factor : 0.1870

ISSN No :2231-5063

Monthly Multidisciplinary Research Journal

Golden Research Thoughts

IMPACT FACTOR : 0.2105

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Golden Research Thoughts
Volume 2, Issue. 9, March. 2013
ISSN:-2231-5063
Available online at www.aygrt.isrj.net

ORIGINAL ARTICLE

A SURVEY OF SECURITY APPROACHES FOR WIRELESS ADHOC NETWORKS

SAAD MASOOD BUTT

Computer and Information Sciences Department,
Universiti Teknologi PETRONAS, Tronoh, Perak, Malaysia

Abstract:

As the popularity of mobile devices and wireless networks significantly increased over the past years. The wireless adhoc network has now become one of the most vibrant and active fields of communication and networking research. These networks are a new generation of networks offering unrestricted mobility without any underlying infrastructure. As their principle application is in disastrous environments, security is critical. Various challenges are faced in the adhoc environment, mostly due to the resource poorness of these networks. One man confront in the design of these networks is their vulnerability to security attacks. The solutions for conventional networks are usually not sufficient to provide efficient adhoc operations. Just because of its wireless nature of communication and lack of any security infrastructure raise several security problems and threats.

In this paper, we briefly review the threats an adhoc network faces and the security goals to be achieved. Moreover, it also presents existing security schemes used in wireless adhoc networks in order to handle security threats.

KEYWORDS:

Adhoc network, Security, IEEE 802.11, Attacks.

INTRODUCTION:

With the advancement in wireless technologies like Bluetooth, IEEE 802.11, a new concept of networking has emerged. This is known as adhoc networking where mobile users arrive within the defined range of the wireless link and participate in setting up the network for communication [1].

Adhoc networks are a new model of wireless communications for wireless hosts or nodes. In an adhoc network there is no supporting infrastructure such as base stations, access points or wireless switching centers.

An adhoc network can be established as soon as two or more nodes are within each other's transmission range. Nodes within range communicate directly, while nodes further apart rely on other nodes to convey messages for them. If the nodes in the network are mobile, then the topology of the network frequently changes [1].

Lack of infrastructural support and susceptible wireless link attacks, security in adhoc networks becomes inherent weakness. Providing adequate security measures for adhoc networks is a challenging task.

One of the challenging issues is dynamic because of frequent changes in both its topology and its

Title : A SURVEY OF SECURITY APPROACHES FOR WIRELESS ADHOC NETWORKS
Source:Golden Research Thoughts [2231-5063]SAAD MASOOD BUTT yr:2013 vol:2 iss:9

membership. Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromise. The dynamic topology and the absence of a supporting infrastructure render most of the existing cryptographic protocols useless as they were not developed for this dynamic environment. It is desirable that security mechanisms should be to adapt on-the-fly to these changes in topology.

Secondly, Wireless communications are easy to intercept. It is also easy to actively insert or modify wireless messages. This means that unprotected wireless networks are open to a wide range of attacks, including node impersonation, message injection, loss of confidentiality, etc.

Thirdly, in many situations the nodes may be left unattended in a hostile environment (e.g., a battlefield). This enables adversaries to capture them and physically attack them. Proper precautions are required to prevent attackers from extracting secret information from them. Even with these precautions, we cannot exclude that a fraction of the nodes may become compromised. This enables attacks launched from within the network.

Finally, an adhoc network may consist of thousands of nodes. So security mechanisms should be scalable to handle such a large network.

Security is as important in adhoc networks as it is important in traditional networks like the Internet. Sensitive data should be protected from malicious eavesdroppers and network services should only be provided to eligible users [2]. As adhoc networks do not have any predefined infrastructure and all network services are configured and created on the fly. Due to this reason security is a critical issue of adhoc networks. Since nodes use the open, shared radio medium in a potentially insecure environment, they are particularly prone to malicious attacks, such as denial of service (DoS). Lack of any centralized network management or certification authority makes the dynamically changing wireless structure very vulnerable to infiltration, eavesdropping, interference.

Based of above mentioned challenges and threats we organize our paper as follows: Section 2 gives the review on wireless adhoc network. Section 3 describes the Security goal to be achieved in wireless adhoc network. Section 4 describes different type of attacks in wireless ah hoc network. Section 5 present types of exiting security schemes for wireless adhoc network and why they are essential for it. Section 6 presents security architectures for wireless ad hoc network. Section 7 concludes the paper.

RELATED WORK

Security in wireless adhoc networks has recently gain a momentum and became a primary concern in attempt to provide secure communication in a hostile wireless adhoc environment. Achieving security performances in wireless adhoc environment is a challenging task. It is difficult to differentiate between malicious network activity and specific problems associated with an adhoc networking environment. In an adhoc network, malicious nodes may enter and may collude with other malicious nodes to disrupt network activity and avoid detection. For this many security schemes have been proposed to deal with security aspects in wireless adhoc networks although neither of them has succeeded to completely achieve all security goals.

Self-securing approach to node authentication in wireless adhoc networks is presented by Haiyun Luo [3]. This approach provides scalable, distributed authentication services in adhoc networks. He designed to takes a self securing approach, in which multiple nodes collaboratively provide authentication services for other nodes in the network. He proposed a localized trust model that lays the foundation for the design, together with its realization to address networking issues of node mobility, network dynamics and wireless channel errors. A scalable share update scheme is developed, and several optimization techniques that greatly enhance the efficiency and robustness of that algorithms and protocols were proposed. Through localized design, he ensured the scalability of the architecture to facilitate practical deployment in a potentially large scale network with dynamic node membership.

Where as Srdjan Capkun [4] have provided a solution to the difficult problem of setting up security associations in wireless adhoc networks. He proposed a technique in which security associations between nodes are established, when they are in the vicinity of each other, by exchanging appropriate cryptographic material. He has illustrated this approach by explaining with two application scenarios: fully self-organized networks and networks with an off-line authority. For the first scenario, he showed that the mechanism is highly understandable by the user, as it reproduces the concept of friends and leverages on physical encounters; these encounters make it possible for a user to associate a face to a given identity (and to a given public key), solving many of the problems of classical security mechanisms. For the second scenario, he showed how adhoc networks that are secured with a central authority can also benefit from mobility. More specifically, a direct establishment of security associations over the one-hop radio link solves the problem known as the security-routing interdependency loop.

SECURITY GOALS

Security is a critical issue of adhoc networks that is still a largely unexplored area. Since nodes use the open, shared radio medium in a potentially insecure environment, they are particularly prone to malicious attacks, such as denial of service (DoS). Lack of any centralized network management or certification authority makes the dynamically changing wireless structure very vulnerable to infiltration, eavesdropping, interference etc. Security is often considered to be the major "roadblock" in commercial application of adhoc network technology.

Security is an important issue for adhoc networks, especially for those security-sensitive applications. To secure an adhoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

Availability ensures the survivability of network services regardless of denial of service attacks. A denial of service attack could be launched at any layer of an adhoc network. On the physical and media access control layers, an opponent could employ congestion to interfere with communication on physical channels. On the network layer, an opponent could disrupt the routing protocol and cut off the network. On the upper layers, an opponent could bring down high-level services. One such target is the key management service, an essential service for any security framework [5].

Confidentiality ensures that certain information is never disclosed to illegal entities. Network transmission of sensitive information, such as strategic or tactical military information, requires secrecy. Leakage of such information to enemies could have shocking consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a field.

Integrity guarantees that a message being transferred is never ruined. A message could be ruined because of benign failures, such as radio transmission impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the uniqueness of the peer node it is communicating with. Without verification, an opponent could impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

Finally, non-repudiation ensures that the source of a message cannot disagree with having sent the message. Non repudiation is useful for exposure and isolation of compromised nodes. When a node A receives an mistaken message from a node B, non-repudiation allows A to accuse B using this message and to encourage other nodes that B is compromised.

Traditional security mechanisms, such as authentication protocols, digital signature, and encryption, still play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in adhoc networks. However, there are other security goals that are of concern to certain applications such as authorization, anonymity, self-stabilization, Byzantine robustness, location privacy, etc [6]. The security of adhoc networks also has to consider features such as privacy, correctness, reliability and fault tolerance.

ATTACKS IN ADHOC NETWORKS

A threat in a communication network is a potential event or series of events that could result in the violation of one or more security goals. The actual implementation of a threat is called attack. Wireless adhoc networks are target for all the threats that occur in fixed networks, i.e., masqueraded identities, authorization violations, eavesdropping, data loss, modified and falsified data units, repudiation of communication processes and sabotage. Moreover, the existence of the wireless transmission links and dynamic network topology contributes considerably towards increasing the threat potential.

Types of Attacks

Attacks against adhoc networks are generally divided into two groups:
Passive attacks (typically involve only one eavesdropping of data)
Active attacks (involve actions performed by adversaries, such as replication, modification and deletion of exchanged data)

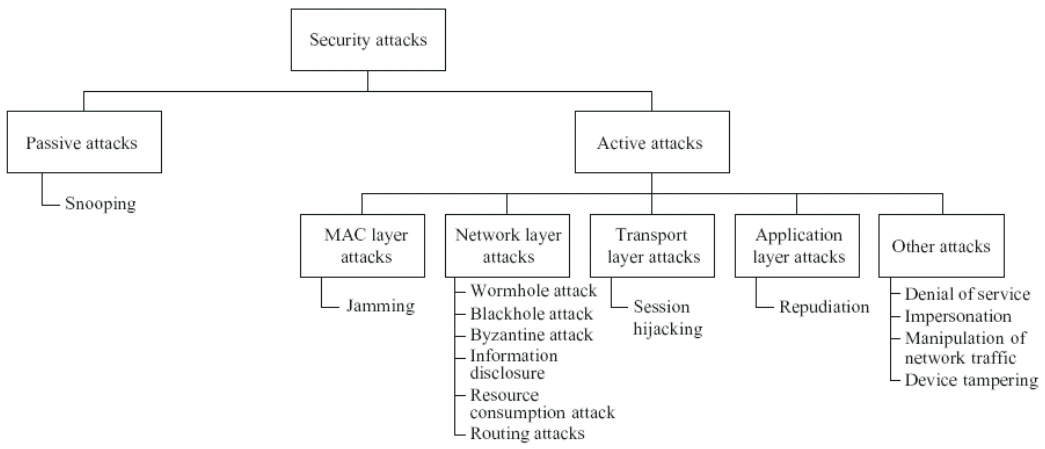
Attacks are considered as external attacks if they are targeted to cause congestion, propagate incorrect routing information, prevent services of working properly or shutdown them completely. External attacks can be active or passive. External active attacks that can be usually easily performed against adhoc network are: black hole, routing table overflow, sleeps deprivation and location disclosure.

External active attacks can usually be prevented by using standard security mechanism such as firewalls, encryption, etc [6].

Internal attacks are more severe attacks, since malicious nodes have already been authorized and are thus protected with the security mechanisms the network and its services offer. These kind of malicious parties are called compromised nodes. They may operate as a group using standard security protection to protect their attacks, compromising the security of the whole adhoc network. Attacks can also be classified as malicious or rational. Malicious attacks aim to harm the members or the functionality of the network, involving any means disregarding corresponding costs and consequences.

According to the affected mechanisms, two levels of attacks can be distinguished:
Attacks on basic mechanisms of adhoc network (e.g., the routing)
Attacks on security mechanisms (e.g., the key management)

Vulnerabilities of the basic mechanisms, include cooperativeness of the nodes (attempt to work according to the rules in order to have fair allocation of resources), node selfishness (deny to relay packets for other nodes in order to save battery), neighbor discovery (as in Bluetooth), etc. Vulnerability of security mechanisms points out the importance of a good cryptographic design with proper management and safe keeping of a small number of cryptographic keys [7]. With node mobility and variable these objectives are not trivial. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious, while nodes that perform passive attacks aiming to save battery life for their own communications are considered selfish. Functionalities of different layers can be threat of different security attacks. Below Figure1 gives a classification of attacks possible in wireless adhoc networks. The following subsections present different types of attacks and the way they compromise security.



Classification of attacks in wireless ad hoc networks

Figure

a.Denial of Service

The denial of service (DoS) can produce a severe security risk in any network. This threat is produced either by unintentional failure or by malicious actions. The consequences strongly depend on particular application. For instance, in the battlefields scenario, the consequences of shutting down the network can be catastrophic, while during the conference connection in the conference room, it may only cause some disturbances. The denial of service attack has many forms. The classical way is to flood any centralized resource, which can disturb its correct operation or completely crash it. Adhoc networks which exist without centralized infrastructure are more sensitive to distributed denial of service attacks. So, if the attackers have enough computing power and bandwidth for their operation, they can easily crash and congest the smaller adhoc networks. Compromised nodes can initiate severe threats to adhoc networks if they are able to modify the routing protocol (or part of it) and send the routing information very frequently.

It can cause congestion or even prevent nodes to gain new routing information about the changed network topology. If the compromised nodes and if the changes of the routing protocol are not detected, the consequences are severe (even the network seems to operate normally). This invalid operation initiated by malicious nodes in adhoc networks is called a Byzantine failure.

b.Impersonation

Impersonation attacks can be serious security risk in adhoc networking, concerning critical operations in all levels. Compromised nodes can masquerade itself as trusted nodes and initiate false or even dangerous behavior such as sending false routing information, gaining access to configuration system as a super-user, certify public key without proper credentials, give false status information to other nodes, etc. Impersonate or masquerade threats are mitigated by applying strong authentication mechanisms. Authentication provides a party to be able to trust the origin of data it receives or stores. It usually is performed in every layer by application of digital signatures or keyed fingerprints over routing messages, different information (configuration or status) or exchanged payload data of the used services. Digital signatures and public-key cryptography requires relatively significant computation power and secure key management, which is inappropriate for wireless adhoc network capabilities. Lighter solutions include keyed hash functions or a priori negotiated and certified keys and session identifiers.

c.Disclosure

Exchanging confidential information must be protected from eavesdropping and unauthorized access. In adhoc networks, confidential information can concern specific status details of a node, location of nodes, private or secret keys, passwords, etc. The disclosure of the exchanged or stored information can be especially critical in military applications.

d.Trust Attacks

Trust is a privilege associated between the identity of the user with particular trust level. So, a trust hierarchy is an explicit representation of trust levels. Attacks on the trust hierarchy can be initiated by inside or outside nodes, if they try to impersonate anyone else and obtain higher level privileges. Different mechanisms can be used to protect against trust attacks, such as strong access control mechanisms (Authentication, Authorization and Accounting or AAA) and cryptographic techniques (encryption, public key certificates, and shared secrets). Some techniques to prevent insider attacks include secure transient association and tamper proof and tamper resistant nodes [6].

e.Attacks on Information in Transit

Compromised or enemy nodes can utilize the information carried in the routing protocol packets to launch attacks. These attacks can cause corruption of the information, disclosure of sensitive information, misusing of the legitimate service from other protocol entities or even denial of service. Threats to information in transit include: interruption, intersection and subversion, modification of the information integrity, and fabrication, i.e., insertion of false routing information.

f.Attacks against Secure Routing

Attacks against secure routing are severe threat to adhoc networks. Internal attacks are difficult to differentiate, because the network topology dynamically changes. Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, fabricating false routing information and by impersonating other nodes. Malicious nodes can easily perpetrate integrity attack, by simply altering protocol fields in order to subvert the traffic. A special case of integrity attack is spoofing. A malicious node impersonates a legitimate node due to the lack of authentication in the current adhoc routing protocols. It can result in miss presentation of network topology and undesirable network loops or network portioning.

Another type of active attack is the creation of a tunnel or wormhole attack. During this attack, two colluding malicious nodes link through a private connection (i.e., tunnel) bypassing the network. This allows a node to short circuit the normal flow of routing messages and create a virtual vertex cut in the network. This is controlled by the two colluding attackers. Lack of cooperation among adhoc nodes due to node selfishness can result in denying participation in routing protocol or forwarding packets. The selfishness problem may cause so called black hole attack [8].

SECURITY SCHEMES IN ADHOC NETWORKS

It is difficult to differentiate between malicious network activity and specific problems associated

with an adhoc networking environment. In an adhoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only occasionally, further complicating their detection. Dynamic topologies make it difficult to obtain a worldwide view of the network and any estimate can become quickly obsolete. Many security schemes have been proposed to deal with security aspects in wireless adhoc networks although neither of them has succeed to completely achieve all security goals.

Link-layer security schemes protect the one-hop connectivity between two direct neighbors that are within communication range of each other through secure MAC (medium access control) protocol. The most prevalent security solutions among wearable wireless devices are presented in data-link-layer security schemes implemented in IEEE 802.11[9] and Bluetooth standards [10]. IEEE 802.11, primarily using vulnerable WEP (wired equivalent privacy)[11], has been enhanced into IEEE 802.11i/WPA version. The Target Group TGi proposed long-term architecture based on IEEE 802.1x that supports various authentication modes. Bluetooth specification includes a set of security profiles for service-level and for data-link-layer security [12].

Particular attention is dedicated to authentication schemes that deal with problems from simple authentication approaches, such as in resurrecting duckling [13], zero configuration (where nodes must be able to authenticate each other without any infrastructure [8]) and face-to-face authentication over short-range link in small spontaneous networks [14], up to the large scale self-organized distribution concepts (for key-based and cryptography-based schemes) and trust graphs which behave like small world graph and appropriate certificate chains necessary to verify any public key. Scalable distributed authentication is achieved in self-securing adhoc wireless networks combined with localized trust model [3].

Cooperative security schemes try to cope with node selfishness in a different way. It proposes and introducing a virtual currency for any transaction in order to motivate node participation. Neighbor's verification of well behaved nodes through token release is implemented in [15].

Secure packet forwarding schemes provide protection against node's failure to correctly forward data packets and consists of detection technique and reaction scheme. An example of localized detection and end-host reaction are watchdog and path rather proposed in [16].

a.Intrusion Detection

Intrusion detection includes capturing audit data and providing evidence if the system is under attack [17]. Based on the type of the used audit data, the intrusion detection system (IDS) can be categorized as network-based and host-based. The former usually runs on the gateway of a network and exams the packets that go through the network hardware interface, while the latter monitors and analyzes the events generated by programs or users on the hosts [18]. The techniques used in intrusion detection systems can be classified as: misuse detection (use patterns of known attacks) and anomaly detection (flag deviation of known attacks). Both techniques rely on sniffing packets and using those packets for analysis [19]. Zhang and Lee [17] in propose architecture for intrusion detection and response where every node in the wireless adhoc network participates in intrusion detection and response through individual IDS agents. Since there are no fixed “concentration points”, where real-time traffic monitoring can be done, audit collection is limited by the radio-range of the devices. Anomalies are not easily distinguishable from localized, incomplete and possibly outdated information which makes anomaly detection schemes not directly applicable in wireless adhoc networks. So, the authors in [17] propose a new architecture for IDS, based on IDS agents. Intrusion detection complements intrusion prevention techniques such as encryption, authentication, secure MAC, secure routing and so on, improving the network security. To be efficient, it should have distributed and cooperative architecture and preferably implement anomaly detection. Further improvement can be achieved if it is incorporated into all networking layers and in an integrated cross-layer manner.

b.Secure Routing in Wireless Adhoc Networks

The routing in wireless adhoc networks can not rely on dedicated routers as in wire line networks. This functionality is spread over all nodes which act as regular terminals as well as routers for other nodes. Providing secure routing in such environment faces many problems specific for adhoc networking and requirements to resist to possible security attacks. Most of the well known routing protocols for adhoc networks do not include security aspects. The protection against vulnerability of wireless adhoc networks from different security attacks and especially attacks at the networking layer must fulfill certain requirements[20].

Severe threat against adhoc routing is the wormhole attack which can completely disable the routing and disrupt the communication. Number of proposals for detection of a wormhole use approach based on packet leashes (e.g., temporal leashes, geographical leashes)

A lot of different approaches are proposed in order to achieve security-aware routing in wireless adhoc networks. They implement different mechanisms such as strong encryption, digital signatures, timestamps, secret-key cryptography, hashing function, MACs, etc. Below Table presents the most important security-aware routing properties and appropriate resolving techniques.

Secure aware routing properties and techniques

Authenticity	Password, certificate
Authorization	Credentials
Integrity	Digest, digital signature
Confidentiality	Encryption
Non-repudiation	Changing of digital signatures
Timeliness	Timestamp
Ordering	Sequence number

Several security routing protocols are briefly discussed in the following subsections.

SRP The secure routing protocol (SRP) can be applied to a multitude of existing reactive routing protocols to protect against attacks that disrupt the route discovery process and guarantee the acquisition of correct topological information [21]. This protocol guarantees that fabricated, compromised or replayed route replies would either be rejected or never reach back to the querying node.

SAR The security aware adhoc routing protocol (SAR) defines level of trust as a metric for routing and as one of the attributes for security which is taken into consideration while routing [22]. Different privileged levels and levels of trust can be defined among the nodes following the desired trust hierarchy. Nodes at each trust level share symmetric keys for encryption/decryption distributing a common key among themselves and with nodes with higher level of trust. However, the protocol requires different keys for different level of security, which increases the total number of keys in the network.

SEAD The secure efficient adhoc distance vector (SEAD) routing protocol is based on the destination-sequenced distance vector (DSDV) routing protocol [23] designed to overcome the DoS and resource computation attacks. SEAD was inspired by DSDV-SQ routing protocol (a beneficial version of DSDV) and deals with the attackers that modify the sequence number and the metric field of a routing table update message. To secure the DSDV-SQ [24] routing protocol, SEAD implements the one-way hash chain and does not rely on expensive asymmetric cryptography. Security mechanisms implemented in SEAD are authentication of sequence number and metric of a routing table update message using hash chain elements. The receiver also authenticates the sender of SEAD routing information in attempt to eliminate malicious nodes (either by implementation of a broadcast authentication mechanism.

ARAN The authenticated routing for adhoc networks (ARAN) routing protocol is based on cryptographic certificates and provides protection against malicious actions carried by third parties and peers in the adhoc environment. The implemented minimum security approach introduces authentication, message integrity and non-repudiation [25] and consists of a preliminary certification process followed by a mandatory end-to-end authentication (and an optional second stage that provides secure shortest path).

ARIADNE On-demand secure routing protocol (ARIADNE) is based on DSR and relies only on highly efficient symmetric cryptography [26]. It needs some mechanism to distribute the authentic keys required by the protocol. Each node needs a shared secret key (between a source and a node), an authentic key for each node in the network and an authentic route discovery chain element for each node. ARIADNE provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key. However, it does not protect against wormhole attacks, except in its advanced version.

S-AODV Security-aware AODV (S-AODV) protocol is an efficient solution to eliminate a black-hole attack caused by a single malicious node [27]. A malicious intermediate node could advertise that it is the shortest path to the destination resulting in the black-hole problem. Proposed solutions deal with limitations in generating a route reply packet or are realized through checking the neighbors of the malicious intermediate node. The S-AODV protocol assumes that each intermediate node can validate all transit routing packets. The originator of a control message appends a RSA signature and the last element of a hash chain. A message traverses the network and the intermediate nodes cryptographically validate the signature and the hash value. S-AODV requires considerable control overhead and is incapable of dealing with malicious nodes that work in a group.

SECURITY ARCHITECTURES FOR ADHOC NETWORKS

Most of the security schemes concentrate on intrusion detection, secure routing, authentication and key management aiming to provide protection against particular security attack or attacks. There are several attempts to provide generic approach defining generic security architectures for wireless adhoc networks which usually jointly considers more than one security schemes. Examples of such approaches are: group collaboration architectures, a general intrusion detection architecture, a subscription less service architecture, Archipelago security architecture, layered architecture, integrated architecture, etc. Following sections give a short description of several such architectures.

Group collaboration security architectures present security models and mechanisms capable of supporting group collaboration in wireless adhoc networks. Short term or long term collaboration and sharing of resources require effective security models that allow such grouping to work. The basic of these models are context sensitive security and developing of object-centered group interaction models for collaboration in wireless adhoc networks. For this security approach many open questions are still under consideration [28].

Hierarchical hybrid networks present security architecture capable of defending against link attacks. Wireless nodes are structured into groups. The security schemes utilize encryption/decryption and public key based authentication techniques [29].

Cluster-based security architecture for securing communication in mobile adhoc networks which is highly adaptable to their characteristics [30]. They divided the network into clusters and implemented a decentralized certification authority. Decentralization is achieved by using threshold cryptography and a network secret distributed over a number of nodes. Different types of keys (symmetric cluster key, asymmetric public key) and certificates can be used in communication. Nodes decide adaptively about the security level and appropriate encryption (no encryption, secret cluster key for intra-cluster only, public node keys directly exchanged or public node keys certified by the cluster head node).

A new framework for multicast (tree-based) security proposed in [31] concerns with the security in large dynamic multicast groups, involving a one-to-many communication pattern, with a dynamic set of recipients. This framework addresses the conflicting requirements (scalability and security) and defines basic properties of set of cryptographic functions that assure confidentiality (either for encryption of bulk data or only for encryption of short messages as required by key distribution) including intermediate components.

CONCLUSION

This paper gives an insight in the security problems and solutions of wireless adhoc networks. Wireless adhoc networks impose additional challenges in front of the designers, due to the lack of infrastructure and the dynamic and ephemeral character of the relationship between the network nodes. They require more sophisticated, efficient and well designed security mechanisms to achieve security goals. Increasing number of adhoc networking applications emphasize a need for strong privacy protection and security mechanisms. Security in adhoc networking is a huge topic and this paper gives an overview of the most relevant issues. It defines security goals and possible threats and attacks, explains major security mechanisms and schemes and presents several security architectures. [32]

There are still many challenges ahead. Security features intend to be embedded in adhoc devices providing secure link layer functionalities. Efficient use of computation resources and guarding against parasitic computation is another challenge. The research in the area of authentication and key management concentrates on designing cryptographic algorithms that should be efficient in sense of computational and message overhead. Variety of broadcast and multicast scenarios are still waiting to be resolved. Designing self-enforcing privacy policies and enhancing privacy mechanisms are challenging issues for ubiquitous computing environments.

ACKNOWLEDGMENTS

We would like to thank Dr. Munir Naveed for his invaluable contributions to this work.

REFERENCES

[1]P. V. Jani," Security within Adhoc Networks", Position Paper, PAMPAS Workshop, Sept. 16/17 2002, London
[2]L. Zhou and Z.J. Haas, "Securing Adhoc Networks", IEEE Networks, 13(6): 24-30, Nov/Dec 1999
[3]H. Luo, Z. P, J. Kong, S. Lu and L. Zhang, "Self securing Adhoc Wirless Netwrok", Proceding ISCC 2002, Seventh International Symposium on Computer and Communation, 1-4 July 2002, ISSN: 1530-1346, INSCEC Accession Number: 7474253, Pages: 567-574, 2002
[4]S. Capkun, J. P. Hubaux and L. Buttyan, "Mobility Helps Security in Adhoc Networks", Proceding of the 4th ACM International Symposium on Mobile Adhc Networking and Computing, ANNAPOLIS, Maryland, USA, Pages: 46-56, 2003
[5]G. Schafer, "Security in Fixed and Wireless Networks", John Wiley and Sons, 2003
[6]Ilyas, M., The Handbook of Adhoc Wireless Networks, CRC Press, 2003.
[7]Karpijoki, V., "Security in Adhoc Networks," Tik-110.501 Seminar on Network Security, 2000
[8]Molva, R. and Michiardi, P., "Security in Adhoc Networks," Personal Wireless Communications (PWC 2003), Venice, Italy, September 2003
[9]IEEE 802.11, Standard Specifications for Wireless Local Area Networks
http://standards.ieee.org/wireless
[10]Bluetooth SIG, Specification of the Bluetooth system, Version 1.1; February 22, 2001, available at https://www.bluetooth.com
[11]ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Authentication and Privacy," 1999
[12]Vanhala, A., "Security in Ad-hoc Networks," Research Seminar on Security in Distributed Systems, Department of Computer Science, University of Helsinki, 2000
[13]Hoeper, K. and Gong, G., "Models of Authentications in Adhoc Networks and Their Related Network Properties," Technical Report CACR 2004-2003, Centre for Applied Cryptographic Research, University of Waterloo, 2004.
[14]Feeney, L. M., Ahlgren, B., Westerlund, A., and Dunkels, A., "Spontnet: Experiences in Configuring and Securing Small Adhoc Networks," Fifth International Workshop on Networked Applicances (IWNA5), Liverpool, UK, October 2002
[15]Buttyan, L. and Hubaux, J. -P., "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Adhoc Networks," Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne, 2001
[16]Michiardi, P. and Molva, R., "Core: A COllaborative REputation mechanism to Enforce Node Cooperation in Mobile Adhoc Networks," IFIP Communication and Multimedia Security Conference, 2002
[17]Zhang, Y. and Lee, W., "Intrusion Detection in Wireless Adhoc Networks," Mobicom'00, Boston, MA, USA, 2000
[18]Wai, F. H., Aye, Y. N., and James, N. H., "Intrusion Detection in Wireless Ad-Hoc Networks," CS4274 Introduction to Mobile Computing, term paper, Fall 2005, School of Computing, National University of Singapore
[19]Anjum, F., Subhadrabandhu, D., and Sarkar, S., "Intrusion Detection for Wireless Adhoc Networks," Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida, October 2003.
[20]Dennis, L. S. E. and Xianhe, E., "Study of Secure Reactive Routing Protocols in Mobile Adhoc Networks," CS4274 Term Paper, School of Computing, National University of Singapore
[21]Papadimitratos, P. and Haas, Z., "Secure Routing for Mobile Adhoc Networks," CNDS, 2002.
[22]Yi, S., Naldurg, P., and Kravets, R., "A Security-Aware Routing Protocol for Wireless Adhoc Networks," 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002
[23]Perkins, C. E. and Bhagwat, P., "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of SIGCOMM 1994, 1994
[24]Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. -C., and Jetcheva, J. G., "A Performance Comparison of Multi-Hop Wireless Adhoc Network Routing Protocols," Proceedings of MOBICOM 1998, 1998.
[25]Dahill, B., et al., "A Secure Protocol for Adhoc Networks," IEEE ICNP, 2002
[26]Hu, Y. -C., Perrig, A., and Johnson, D. B., "Ariadne: A secure On-Demand Routing Protocol for Adhoc Networks," Proceedings of MOBICOM 2002, 2002

[27]Patwardhan, A., Parker, J., Joshi, A., Karygiannis, A., and Iorga, M., "Secure Routing and Intrusion Detection in Adhoc Networks," 3rd IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 2005
[28]Berket, K. and Agarwal, D., "Enabling Secure Ad-hoc Collaboration," WACE03, Seattle, Washington, USA, June 2003
[29]Lu, Y., Bhargava, B., and Hefeeda, M., "An Architecture for Secure Wireless Networking," Available at: http://www.cs.purdue.edu/homes/yilu/papers/wireless-sec.pdf
[30]Bechler, M., Hof, H. -J., Kraft, D., Pahlke, F., and Wolf, L., "A Cluster-Based Security Architecture for Adhoc Networks," IEEE INFOCOM 2004, Hong Kong, March 2004
[31]Molva, R. and Pannetrat, A., "Scalable Multicast Security with Dynamic Recipient Groups," ACM Transactions on Information and System Security, 3, August 2000, pp. 136–160
[32]Wrona, K., "Distributed Security: Adhoc Networks & Beyond," PAMPAS Workshop, London, September 2002

SAAD MASOOD BUTT received his BS (Software Engineering) degree from Bahria University Islamabad, Pakistan in 2008. He completed his MS (Software Engineering) degree in 2010 from Bahria University Islamabad, Islamabad Pakistan. He is the recognized Engineer of Pakistan approved by Higher Education Commission and Pakistan Engineering Council (PEC). He has got more than 4 years' experience and was associated with various organizations in Pakistan. Currently, he is pursuing his PhD degree in the department of Computer and Information Sciences at Universiti Teknologi PETRONAS, Malaysia.