Ad hoc Network and its Security Essentials

Monika Kohli
Department of Computer Engineering & Information Technology
K. J. Institute of Engineering. & Technology
Savli, Vadodara, Gujarat, India
monika.mann@gmail.com

Abstract—This In this paper we present an analysis of ad hoc network and how the attacks are prominence on the ad hoc network. Basically ad hoc network is a combination of several nodes which are linked over without wires which means wireless medium is used for this topology. In addition, ad hoc networks are design for particular environment even though it works in most difficult surrounds. Security aspects are more new in ad hoc networks as compares to old networks, still ad hoc networks are faces many security problems in current scenario. Due to the environment specific nature of the ad hoc networks its implementation is not as easy as we think. In this article we also discuss some security attacks.

Keywords- Ad hoc Network, Nodes, Networking, Security Attacks

I. INTRODUCTION

An ad hoc network is group of many nodes which are interconnected through wireless way. An ad hoc network can be designed together and separate network without follow specific infrastructure to accomplish the process. In ad hoc network nodes are often use such an mobile because it put on in such a manner in which wireless medium is used for communication, in such a scenario network are known as mobile ad hoc network. it is not necessary that mobile node is compulsory used as requirement of ad hoc network, in ad hoc network we can also use fixed and under wired nodes, that are used in operation in infrastructure which is specific. The security essentials in ad hoc networks are not usable those are appropriate in old networks. In ad hoc network the main security necessities like privacy plus authenticity still not complete. The node processing is more difficult in ad hoc network.

The paper is organized into five segments as follows; segments1 introduces the introduction about ad hoc networks. Segments 2 introduce the networking operations which are applicable in ad hoc networks. A segment 3 discusses the attacks on ad hoc networks. Segments 4 represent criteria for protecting Ad Hoc Networks. Segment 5 concludes the conclusion about the given statements.

II. AD HOC NETWORK-INSIGHT

A. What is Ad hoc Network

An ad hoc network is a combination of many nodes which are connected through without wires that means wireless medium is used for this topology. But in the wired medium ad hoc networking is also possible, in which many nodes are used for this network implementation.

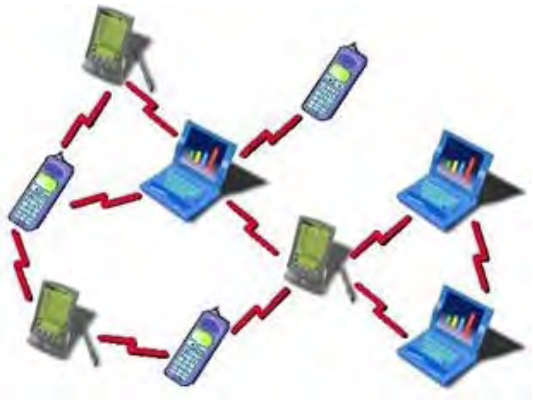

Figure 1. Ad hoc Network

Nodes are collection of minute devices that are producing a computable response from physical or non-physical environmental circumstance by different deviations. Nodes are low power consumption devices which consists one or more sensors, a processor, a power supply, radio, an actuator and memory [4].

There are four elementary constituents in a sensor network, first one is an assembly of distributed or localized nodes; the second is an interconnecting network that are usually, but not always, wireless based network; third

one is a central point of information clustering and fourth and last is a set of computing resources at the central point or beyond to control data association, event trending, status inquiring, and data mining [3].

B. Mobile Ad hoc Architecture

The Ad hoc network architecture of mobile in which node is used as mobile; hence it is called as the mobile ad hoc network. Here as we can see in the figure that the PDA's are connected to mobile devices, which are in turn connected to proxy nodes denoted as P1, P2 and P3 in the figure. These proxy nodes are connected to wired collection of servers, denoted as wired grids A and B. Between mobiles, PDAs and proxy nodes (these all form a wireless network) are exchanging DICHOTOMY & BoTDP messages (denoted as solid lines in the figure), while between proxy nodes and wired grids MDS, GRAM & GridFTP messages (denoted as dashed lines in the figure) are exchanged. Wired network can also be used between mobile devices communication, instead of wireless communication shown in the diagram.

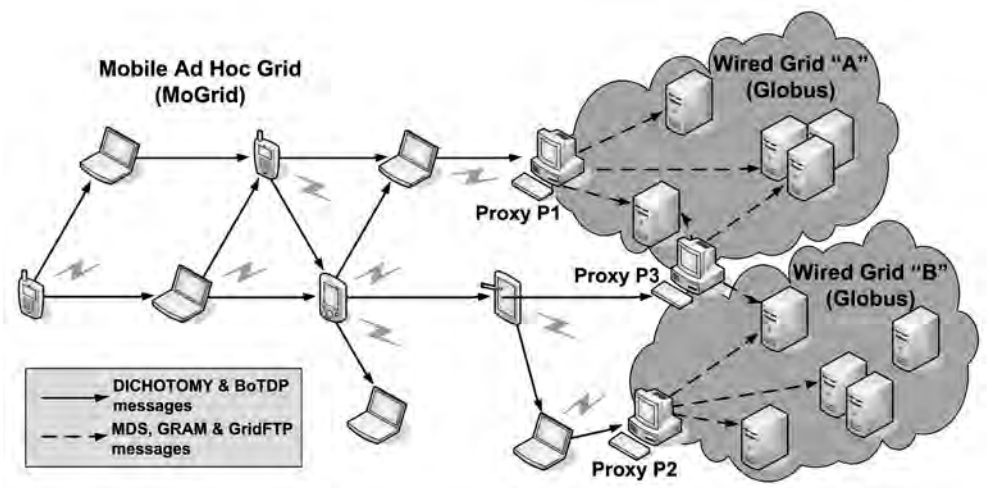

Figure 2. Mobile Ad Hoc Architecture

III. NETWORKING ACTION

Recently, there are two networking operations one is routing and other is network management. Routing protocol classified into three different categories; first is proactive second is reactive and last is hybrid protocols, there all are depends on their topologies.

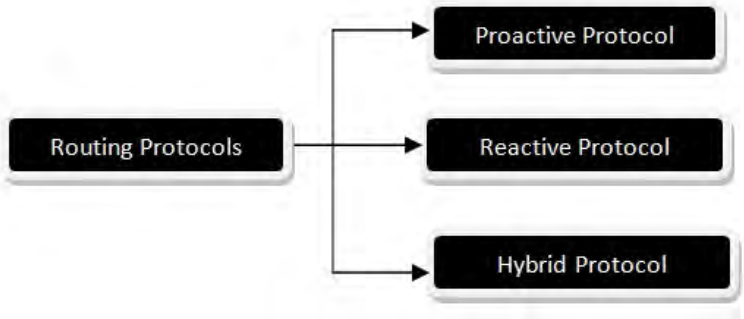

Figure 3. Routing Protocols

1) Proactive protocols is basically distance vector and table driven protocols they may like several old protocols.in which nodes of the protocol are continually change according to the previous routing information therefore each node can instantly process with reliable and up to date routing stands at whatever time there is information's to be transferred.
2) Reactive protocol also known as source initiated on demand protocols. It is not update the information after the time interval. It is circulated to the nodes simply when it required. Several mobile routing protocols are on demand driven for optimizing purposes. It has one drawback such as it creates much overhead while route is identified. So in this case the up to date route is not available when it required for it.
3) A hybrid protocol is combination of both protocols proactive protocols and reactive protocols. They are work between reactive proactive as well as reactive protocols. Even table driven protocols are used between networks and on demand protocols are used inside the networks or vice versa [17]. It

looks like given network not completely proactive or completely reactive. In which the protection of traffic is important in environment that is not secure, so the information regarding communicating party is not disclose to not authorize parties.

Network management consists of the configuration of the nodes in the network like router, client and vital management server. The administration process can be done in manual or automatic manner, it depend on given problem. Network management also include the dynamic configuration regarding the information that is processes in the network while they operate. Network management can be any kind of data which is important information, are protected by unauthorized parties.

IV. AD HOC NETWORK ATTACKS

There are several types of attacks on ad hoc network which are described as follows:

1) *Location Disclosure:* Location disclosure is an attack which points confidentiality requirements of an ad hoc network.by the usage of traffic examination techniques and with simple searching and checking methods, an attackers are able to determine the position of a node, and also the organization of the complete network.
2) *Routing Table Poisoning:* As we know that some tables are managed by Routing protocols in which the information related to the routes of the communication network is stored. In case of poisoning attacks a fabricated signalling traffic is produced and forwarded by the malevolent nodes or such nodes might alter genuine communications coming from other nodes. And this all is done to make some incorrect insertion of data in the tables of the contributing nodes [6].
3) *Breaking the neighbour relationship:* In this attack the invader inserts a smart filter over the communication link among two Information Systems. The statistics in the routing updates can be modified or changed by this filter or the traffic related to any data session can also be captured by this filter.
4) *Denial of Service (DOS):* Wireless Denial of Service is produced by the unpremeditated failure of nodes. DOS attacks exhaust the resources of the target victim node by transferring unnecessary excessive packets, hence preventing the network from accessing services. Numerous DOS attacks might be executed in WSN in different layers [4].
5) *Wormhole:* In the case of a wormhole attack, rivals work together to deliver a low latency side channel for communication [4]. It can be better understood with the scenario discussed here. Suppose there are two attackers, who may own an additional radio for communicating over a higher speed and a long range link.

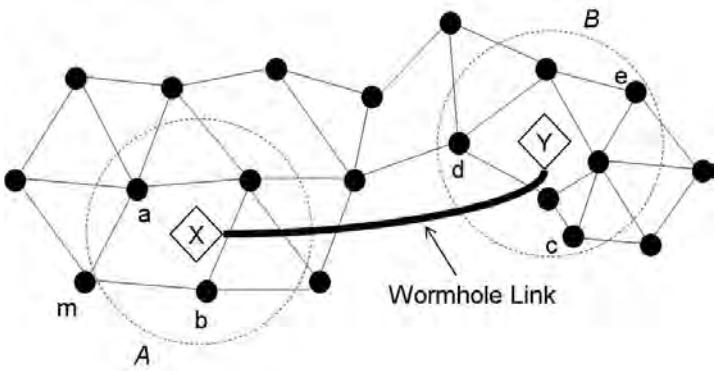

Figure 4. Wormhole Attack

One attacker will relay the message received by him, to the other via the side channel. In this side channel, the messages are communicated as if these are only one node away from the original source. Because it minimizes the distance between two adjacent nodes, it might be the reason for adjacent nodes to favour the attacker for a wormhole attack. Services will not be denied, but the same will be improved provided that the side channel is present. Though, the network will enter and remain in an unpredictable state that requires re-initialization of some services to bring back into appropriate function, when the attacker moves or stops to tunnel messages [4].

6) *Black Hole (Sink Hole):* In Black Hole attacks, a compromised node is made to look exclusively attractive to its neighbouring nodes regarding the routing algorithm and pull almost all of the traffic from a specific area via the compromised node this process creates a symbolic sinkhole with the adversary at the centre [4]. As the nodes near or on the path of packet have countless opportunities to

damage the application data, sinkhole attacks may empower various other threats e.g. selective forwarding.

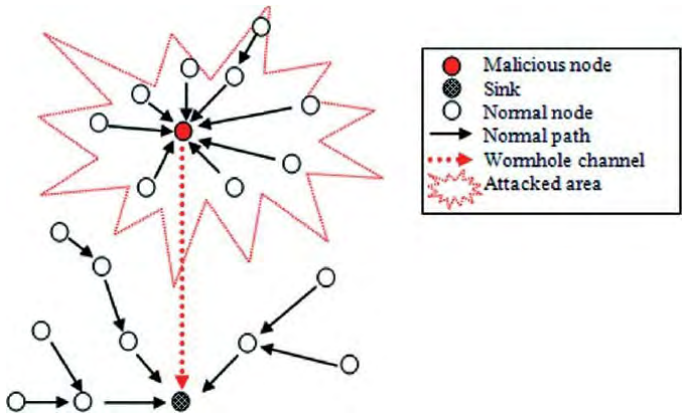

Figure 5. Black Hole Attack

1) *Replay:* In replay attack the attacker inserts into the network routing traffic which is seized earlier. This is the attack which points to the fresh route in the network and it also affect to the poor network security measures.
2) *Blackmail:* Blackmail attack can be called pertinent in contrast to routing protocols that practice the methods required for the identification of malevolent nodes and broadcast communications that attempt to blacklist or boycott the offender. Such reporting communications might be fabricated by an invader and he or she might attempt to segregate sincere nodes from the communication network. In such scenarios, the security characteristics of non-refutation can be useful as it binds a node to the communications generated by the same node.

V. AD HOC NETWORK: PROTECTING MEASURES

Following are the protecting measures for ad hoc networks:

A. Network Operations Security

The protection in the Link or Network layer is the foundation for the security of ad hoc networks. The link layer proposes, in a few ad hoc implementations, resilient security amenities for defending privacy and genuineness, in which case all of the security necessities essentially not to be addressed in the network or its higher layers. As digital signatures are used for authorizing the source of the data and its integrity, the Authenticity and integrity are generally managed simultaneously with routing information. If there is not any integrity protection then the attacker is able to destroy the information or it may be edit the information and it can be able to produce not genuine traffic so the task is separated from the hardware default. In this authenticity is necessary for routing information because source will be able to know the change of routing information. The impersonation attacks could be happen if the authenticity is not definite.

B. Key Management Security

In ad hoc networks the security depends on the use of appropriate management of keys in the system. The system is needs of secrete key and public keys. If public key cryptography is used then complete protection mechanism depend on the security of the secret key. As far the physical security of the node may be reduced. For node confidentially secret key have to be store, which are encrypted by system key [11]. Ad hoc networks which are dynamic the security of the secret key is definite with appropriate hardware safety or by the distribution of key in several nodes. In Ad hoc networks hardware protection is never alone an acceptable explanation for preventing attacks

C. Physical Security

As compared to the wired nodes in conventional networks, the mobile nodes in an ad hoc network are naturally and considerably more vulnerable to physical attacks. Although it is always the ad hoc networking methodology and the surroundings in which the node operates, are the deciding factors on which the significance of the physical security in the whole safeguard of the network is extremely reliant on.

D. Service Aspects

Ad hoc network are applicable for both flat as well as hierarchical infrastructure. In flat infrastructure connectivity of the nodes are straight maintained by themselves.in which the network are not depends on any kind of centralization. In such a network all necessary services like routing of packets and management of key have to be spread so several nodes are responsible for providing service. There is no dedicated server nodes are available in the network, any nodes gives the service to the other node. Some nodes are crash in the network due

to the tolerance. In ad hoc networks redundancy in communication channels may raise the possibility that every node can accept suitable routing data. The denial of service threat may decrease due to the use of redundancy in communication channel.

VI. CONCLUSIONS

In this paper, initially we have discussed some fundamental aspects of an ad hoc network. We have then put some light on the network operations for ad hoc networks and also discussed security attacks on an ad hoc network. Finally we concluded our paper with an overview over protecting measures for an ad hoc network. Ad hoc networking is quiet a fresh area of research where there are many problems related to network security that exist in such networks. We have put our understanding towards the protection measures which should be taken care while dealing with attacks over ad hoc networks. Networks like ad hoc are equipped with speed, ease and flexibility, so that these networks can be applied to a wide range of application fields. This is because we can san ad hoc network and other such networks are always quite open and interesting for research.

ACKNOWLEDGMENT

This work was supported by Dr. Ashok Kumar Jetawat, the author thank to, for his kind guidance in the research and as reviewer to this research paper.

REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
[4] Monika Kohli and Rohit Tiwari, "Security Aspects for Wireless Sensor Network", IJERT, Vol. 1 Issue 8, October – 2012 ISSN: 2278-0181
[5] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[6] [6] Perkins, C. Mobile networking in the Internet. Mobile Networks and Applications 3, 1998, p. 319-334. [referred 25.9.2000] <http://www.baltzer.nl/monet/articlesfree/1998/3-4/mnt071.
[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[8] Wang et al. Secure Routing Protocols: Theory and Practice. North Carolina State University, 2000. [referred 25.9.2000] <http://www.cis.udel.edu/~cshen/859_spring00/paper/CCR-SecureRP2.ps.gz
[9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[10] Bissias, G.D., Liberatore, M., Jensen, D., Levine, B.N., "Privacy vulnerabilities in encrypted HTTP streams" In Proc. Privacy Enhancing Technologies Workshop (PET 2005).
[11] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, "Self-securing Ad Hoc Wireless Networks", 7th IEEE Symp. on Comp. and Communications (ISCC), Taormina, 2002..
[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.
[13] Huaizhi Li, Mukesh Singha, "Trust Management in Distributed Systems" IEEE Computer Society February 2007.
[14] I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. MobiCom, 2004.
[15] J. Nam, S. Cho, S. Kim, and D. Won, "Simple and Efficient Group Key Agreement Based on Factoring" Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '04), pp. 645-654, 2004.
[16] J. Parker, J. L. Undercoffer, J. Pinkston, and A. Joshi., "On Intrusion Detection in Mobile Ad Hoc Networks". In 23rd IEEE International Performance Computing and Communications Conference Workshop on Information Assurance. IEEE, April 2004.
[17] Jeremy J. Blum, Member, IEEE, and Azim Eskandarian, Member, IEEE, "A Reliable Link- Layer Protocol for Robust and Scalable Intervehicle Communications" IEEE Transactions On Intelligent Transportation Systems, vol. 8, no. 1, March 2007.
[18] Jung-San Lee, Chin-Chen Chang, "Secure communications for cluster-based ad hoc networks using node identities" Journal of Network and Computer Applications 22 October 2006
[19] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in Proc. of the IEEE CS Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, Jan. 2003.
[20] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," In Theory and Application of Cryptographic Techniques, p. 344–359, 1993.