Agent Technology and MANET

Ad hoc is determined as a connection method involving network, and is associated with wireless devices in the majority of cases. There is no need in base station for the device to function efficiently, as well as effectively. One session is the exact duration that is established by the connection. Instead of the base stations, Ad hoc devices are capable of detecting other similar devices that fall under Mobile Ad hoc Networks (MANETs). Ad hoc devices accomplish searching and identifying specific nodes that exist in the network system, flooding by the application of some broadcasts brought forward from these nodes. These Ad hoc connections have multiple applications (Vaidy 25).

The main purpose of MANET is to support powerful and efficient operation in mobile wireless networks. It incorporates routine series of operations performed by mobile node, which is the joint between main elements of the network. All terminals of connection are enclosed in a circle. This union is a result of a typology of arbitrary nature. These routers are capable of an accidental organization achieved through a free and random movement. The topology formed by wireless networks is quite unstable and, therefore, unpredictable due to the fact the rapid transformations are expected all the time. The roaming host can be connected to Internet by means of different devices. It may be straightly connected to the definite network segment or via a wireless modem, dial up devise, etc. The basic component of Mobile Ad hoc Networks operation is a wireless node capable of being a sender at one time, a receiver at another time or even a router. At the time the node is sending, messages can be received at specific destinations, as has been directed through the use of some route. When the node is functioning to receive messages, then any node can be the source of the message. At the time the node is functioning as a router it serves to retransmit messages to the particular destination. Although these nodes are rapidly-changing and random, the messages arrive on time to its recipient. They can be discovered in various locations such as planes, boats, cars, houses, and are multiple hosts per one router (Vaidy 27-28).

By Corson and Macker, MANET is an autonomous system of mobile nodes that may function in isolation, or is probable to attain some getaways to and interface with already arranged network (11). A typical MANET exhibits some certain features. The most distinctive is the absence of routing support for mobile host; at the same time other mobile networks are equipped with some base stations. MANET functions for the purpose of accessing the desired destinations as well as servers that are deployed to facilitate the functioning of the network. All nodes have the capability of being routers whereas all of these devices that are wireless have an interconnection amongst themselves and the entire network does not have a central connection. The nodes, therefore, are solely responsible to deliver messages, as well as discovering the topology due to self configuration nature of this network (Corson and Macker 11-12).

The topology exhibited by MANET is dynamic and the nodes have the freedom of an arbitrary movement. This movement is a fundamental part because the rapid changes in the network topology cannot be easily predicted. The network is able to locate alternative pathways automatically by enhancing forwarding of the data through multiple paths through the application of diverse routing mechanisms (Corson and Macker 11-12).

The operation of MANET is energy constrained. The nodes are charged from battery or by other exhaustible energy means, and therefore the need for the conservation of power is an important aspect when this network is concerned.

MANET is basically associated with limited security. Wireless networks are mobile, thus they are exposed to threats of f physical security, cases of interception, can be denied by necessary services. All together it makes MANET more uncertain compared to other networks operating by means of cable connection (Corson and Macker 13).

THE SECURITY AND VULNERABILITY

Its security is an essential component for the basic net functioning. It may be relatively easy to detect network traffic, or retransmit messages within wireless network that has no suitable security protection elements. On the contrary, other networks use the specialized units for the support of their base functions; in Mobile Ad hoc Networks they are performed by all accessible nodes. This essential difference lies on the level of the core of the problems of protection, which are specific in ad-hoc networks. The nodes of ad-hoc network cannot be entrusted to the specialized nodes of classical network, and it cannot be guaranteed, that they will correctly fulfill critical net functions (Siddhartha and Mukesh 17).

TYPICAL REALIZATION

When the hardware protected from the unskillful rotation, and a strict identification infrastructure are not available, for example, in the open environment where the general authority which regulates network does not exist, any unit of ad-hoc of network can be subjected to danger. The correct operation of network requires not only the correct fulfillment of critical net functions by each participating node, but it also requires each node to carry out the clearly specific portion from these functions (Yan 56).

However, the threats are not limited only to harmful intentions and the new type of abnormal behavior, called as selfishness; when the nodes cease interacting, it indicates a probably trouble. In fact, the existing ad-hoc protocols of routing undergo two types of attacks: active attacks and passive attacks. Attack is considered to be active, when the anomalously leading node bears some power expenditures at the time when some threat is constituted. Passive attacks occur mainly because of the absence of collaboration for the purpose of energy conservation (Yan 57).

The nodes, which carry out active attacks, effect the damaging of other nodes. This further leads network failure. These are considered as malicious, while nodes, which carry out passive attacks for the purpose of the retention of the period of battery service for their own interactions, are regarded to be selfish (Yan 58).

The malicious nodes can destroy the correct functioning of the routing protocol, changing routing information, fabricating false routing and playing the role of other nodes. Furthermore, there are also attacks, which are called worm hole. On the other side, selfish units can substantially weaken net productivity and, eventually, divide network simply without participating in the net operations (Yan 58).

Problems

As long as many of the attacks on the wireless networks are similar to the attacks on standard networks, MANET networks are located in larger danger. One of the largest problems is WEP (Wired Equivalent Privacy), standard encrypting data for wireless networks (Yang 133).

One can discover several vulnerabilities in WEP, which makes it possible to break through the network in short period of time. Another problem is associated with open nature of MANET. Because of the special features of wireless networks, it is complicated to control the region of the signal accessibility. Moreover, the signal strength varies, from high to low, depending on the area (Yang 133).

In contrast to simple networks, in MANET a hacker can control or overhear network from locations, which were not intended for maintenance, when network was created. MANET also can be used for creating backdoors for standard networks. Many organizations spend thousands and even millions of dollars for guaranteeing the protection of standard networks, but it is sufficient for only one unscrupulous or uninformed wireless user, connected to the standard network; and it is possible to easily create backdoor, which circumvents all complex and expensive protective systems, thus the hacker easily obtains the access to the thoroughly closed network. This is why, all properties of safety, characteristic of standard networks, are inherent in wireless networks (Yang 134-135).

Threats

There are many potential threats for MANET, such as denial of service (DOS), session taken over and sniffing, which is defined as overhearing of net traffic. The utilities for sniffing appeared from the first days of appearance of most local networks and were intended for facilitating network administration. However, in appropriate hands these utilities – sniffers- became powerful tools for hackers, which make it possible to intercept passwords and other information, transferred by the local network (Yue 75).

Sniffers are traditionally considered as sufficiently complex utilities, which require specific skills for working with them, and often they require complex management. The situation has been changed drastically within the pas few years, when there appeared to be and became easily adopted in use specialized sniffers of passwords. Many of these utilities, referred to the new generation tools, are freely accessible in Internet. Having the built-in data base, sniffers can be easily detected. It's no doubt, that any hacker understands the majority of net protocols by separating the required information, such as bond of usernames and passwords from the rest of data, and breaks into the wireless network (Yue 75-76).

Conclusion and Suggestions

Mobile ad-hoc network is the key factor in the development of wireless communications. These networks inherit the traditional problems of wireless and mobile connection, such as the optimization of capacity, the control of power, improvement in the quality of transmission of data. Furthermore, their multilink nature and probable absence of stable structure introduce the new aspects of studies, such as line pattern, the detection of device, support of typology, and also ad-hoc- addressing and internal control of routing. Routing is the basis of network infrastructure. It controls and governs the flow of communications in the network. In order to establish and support the improved] net topology, routers exchange reports about the state of the connections, its cost and metrics (Siddhartha and Mukesh 24).

For wireless Ad Hoc networks a deficiency in the support of fixed infrastructures and frequent changes in the network typology creates the problems of safe routing more complex. In Ad Hoc networks there is a shortage of the resources of power. Cryptography based on the basis of the open keys is too expensive. But problem consists in how safe connections between the source and the receiver can be established will be before the route between them is established. That could be a topic for further researches in that field (Siddhartha and Mukesh 24).

Works Cited

Corson, Scott, and Josef Macker. *Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations.* Washington: University of Maryland. Naval Research Laboratory, 1999.

Siddhartha, Gupte, and Mukesh Singhal. *Secure Routing in Mobile Wireless Ad Hoc Networks.* June 2004. Sept. 2008 <http://cs.engr.uky.edu/singhal/CS685-papers/adhoc-net.pdf>.

Vaidy, Sunderam S. *Computation Science*. New Mexico: Springer, 2005.

Yan, Zhang. *Wireless Security.* Hershey; New York; London: IGI, Global Information Science, 2008.

Yang, Xiao. *Security in Sensor Network*. Florida: CRC Press, 2006.

Yue, Hao. *Computation Intelligence and Security*. Basel: Birkhauser, 2005.