International Journal of Electrical & Electronics Research (IJEER)
Volume-1, Issue-1, Pages 8-12, June 2013, ISSN: 2347-470X

Challenges in Mobile Ad Hoc Network for Secure Data Transmission

Rahul Misra
M. Tech Scholar
Department of Electronics & Comm.
MITS, Gwalior (MP), India
misra.rahul@gmail.com

Prashant Sharma
M. Tech Scholar
Department of Electronics & Comm.
MITS, Gwalior (MP), India
prashants158@gmail.com

ABSTRACT

An ad-hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. LAR is an on-demand protocol who is based on the DSR (Dynamic Source Routing). The Location Aided Routing protocol uses location information to reduce routing overhead of the ad-hoc network! Normally the LAR protocol uses the GPS (Global Positioning System) to get these location information's. With the availability of GPS, the mobile hosts knows there physical location. Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA), packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program [11]. Ad hoc networks have play an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program [12] and the near-term digital radio (NTDR) program [13]. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available. Since their emergence in 1970's, wireless networks have become increasingly popular in the communication industry. These networks provide mobile users with ubiquitous computing capability and information access regardless of the user's location. paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks - multiple routes between nodes to defend routing against denial of service attacks.

Keywords

LAR, DSR, MANETs, Hand-off, self-organization.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks.

There are currently two variations of mobile wireless networks: infrastructure and infrastructure less networks. The **infrastructure networks** have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A **"Hand-off"** occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone. The other type of wireless network, **infrastructure less networks**, is knows as **Mobile Ad-hoc Networks (MANET).** These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move freely. In this type of networks, some pairs of terminals may not be able to communicate directly with each other and have to rely on some terminals so that the messages are delivered to their destinations. Such networks are often referred to as **multi-hop** or **store-and forward** networks. The nodes of these networks function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices. Mobile Ad-hoc Networks are supposed to be used for disaster recovery, battlefield communications, and rescue operations when the wired network is not available. It can provide a feasible means for ground communications and information access.

2. Characters and Fundamental Challenges of Wireless Ad-hoc Networks

Since Wireless Ad-hoc Networks are inherently different from the well-known wired networks, it is an absolutely new architecture. Thus some challenges raise from the two key aspects: **self-organization** and **wireless transport of information**. First of all, since the nodes in a Wireless Ad-hoc Network are free to move arbitrarily at any time. So the networks topology of MANET may change randomly and rapidly at unpredictable times. This makes routing difficult because the topology is constantly changing and nodes cannot be assumed to have persistent data storage. In the worst case, we do not even know whether the node will still remain next minute, because the node will leave the network at any minute. Bandwidth constrained is also a big challenge. Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple accesses, fading, noise, and interference conditions etc. the wireless links have low throughput. Energy constrained operation. Some or all of the nodes in a MANET may rely on batteries. In this scenario, energy conservation is the most important system design criteria for optimization. Mobile networks are generally more prone to physical security threats than are fixed cable networks. There are increased possibilities of eavesdropping, spoofing and denial-of-service attacks in these networks.

3. The Argument

It is debated in academic as whether the Mobile Ad hoc Networks are a fundamentally flawed architecture. The reason for the debate is that Mobile Ad hoc networks are almost never used in practice, the wireless networks we use now is still Base-station or Access Point related. If we could proof that, technically, the Mobile Ad-hoc is unrealizable, then we could say it is a flawed architecture. We take the position that MANET is a flawed architecture and will prove our position in section 5.

4. Counter Argument

It is claimed that Mobile Ad-hoc networks is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. It is great importance in situation where it is very difficult to provide the necessary infrastructure. Furthermore, ad-hoc networks have been recognized as an important form of wireless network. MANETs are internetworks formed by mobile wireless routers, with each router having one or more associated host devices (e.g., computers and sensors). A MANET's router implements routing protocols that—unlike conventional routing techniques—tolerate rapid changes in connectivity among nodes. MANET's routing algorithms organize the network by automatically discovering the topology of the connectivity among constituent nodes. The collection of interconnected nodes serves as the network's communications infrastructure. MANETs are **non-hierarchical systems**, with each node (mobile router) serving identical roles as a source, sink, and pass-through for data. Thus,

the MANET is not tied to an existing or static communications infrastructure (as is a cellular telephone network).The ability to independently self-organize and serve as its own infrastructure makes MANETs particularly attractive for the industrial communications requirements in harsh manufacturing environments. Many researchers have been done on all aspects of the Mobile Ad-hoc Networks to make it more suitable for wireless communications. People develop lots of routing protocols to fit the mobility of the Wireless Ad-hoc Networks. The routing algorithms become more and more fit the rapid changing network topology of Wireless Ad-hoc Networks. The Wireless Ad-hoc Networks itself is not hierarchy. In order to manage all the nodes and make Routing Protocols as well as Collision Detection mechanism easier, People bring out the idea of constructing the Wireless Ad-hoc Networks into a hierarchic architecture. Thus we have the definition of Cluster. The networks is divided into **clusters**, each cluster has its own cluster head. The cluster head will contain the information of the other nodes in this cluster. This idea is great, by using cluster; we avoid the flooding process when doing routing and fault diagnoses. And also the self-organization method was explored. **Self organization networks** are improved Mobile Ad-hoc networks. They distinguish themselves from traditional mobile ad-hoc networks, based on the traditional internet two level hierarchy routing architecture, by emphasizing their self-organization peculiarities. Self-organized networks can act in an independent way from any provider. Self-organized networks are also potentially very large and not regularly distributed. For example, one single network can cover the entire world. Also, self-organized networks are highly co-operative, the tasks at any layer are distributed over the nodes and any operation is the results of the cooperation of a group of nodes. People believe that MANET will be the main architecture of the future wireless networks where the normal wireless networks are impossible to build, especially in military usage or emergency. They think the most important characteristic which sets Wireless Ad-hoc networks apart from cellular networks is the fact that they do not rely on a fixed infrastructure. They also think Mobile Ad-hoc networks are very attractive for tactical communication in military and law enforcement. Again, they believe that Wireless Ad hoc Networks will play an important role not only in military and emergency application, but also can be applied in civilian forums such as convention centers, conferences, and electronic classroom.

However, we do not agree with the above statements. Our point of view is that when we talk about the Mobile Ad-hoc networks, we think they are a flawed architecture, because **first**, until now, we haven't seen any practice of the Wireless Ad-hoc Networks, are the routing protocols, self-organization, security solutions are all theories based on simulation. **Second**, today, almost every wireless network nodes communicate to base-stations and access points, instead of co-operating to forward packets hop-by hop.

5. Wireless Ad-hoc Networks Issues

Even the most zealot supporters of MANET have to admit that it is a challenging task to enable fast and reliable communication within such a network. The inherent characters of MANET make it a flawed architecture no matter what we have one is will do to improve the performance of the networks. Below are the factors that prevent the mobile ad hoc networks to be an in-flawed architecture.

5.1 Security in Wireless Ad-hoc Networks

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks. This is due to **system constraints** in mobile devices as well as **frequent topology changes** in the Wireless networks. Here, **system constraints include low-power, small memory and bandwidth, and low battery power.** Mobility of relaying nodes and the fragility or routes turn Wireless Ad-hoc Network architecture into highly hazardous architectures. No entity is ensured to be present at every time and it is then impossible to rely on a centralized architecture that could realize network structure or even authentication. It is true that Mobile Ad hoc Networks come from the military. But perhaps those persons forgot one of the most important things: the Security!

Everybody knows that the core requirement for military applications dealing with trust and security! That is to say, security is the most important issue for ad hoc networks, especially for those security sensitive applications. As we have mentioned before, in Mobile Ad-hoc Networks, security is difficult to implement because of the networks constrains and the rapidly topology changes. After investigation, we found that there are two kinds of **security related problems** in the Mobile Ad-hoc Networks. **One** is the attacks based on the networks which are just similar to the Internet, the **other** is Fault Diagnoses. **Fault Diagnoses algorithm** is used to pick out the faulty nodes and at the same time remove the node from the whole networks. This process should be real-time as to guarantee the performance of the whole networks. In order to solve the fault diagnoses problem, many fault diagnoses algorithms were bring out. After carefully surveying the existing algorithm today, we found that they cannot correctly diagnose faulty node with the presence of the changing of the network topology during the process of diagnosis, and these algorithms are analyzed with repetitious diagnosis for all the mobile hosts and cause the great system overhead due to the transmission of diagnosis messages by means of flooding throughout the whole networks. While the topology of Mobile Ad-hoc Networks changes from time to time, then we cannot use this kind of Fault Diagnoses Algorithm to solve the questions. Therefore, we can see that the current fault diagnosis algorithms cannot solve the fault diagnosis problem. As for the networks attacks, there are several **factors of security** that we should consider. First, ***Availability*** ensures the survivability of network services despite denial of service attacks. ***Confidentiality*** ensures that certain information is never disclosed to unauthorized entities. ***Integrity*** guarantees that a message being transferred is never corrupted. ***Authentication*** enables a node to ensure the identity of the peer node it is communicating with. Yet, active attacks might allow the adversary to delete massages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Although that many security-related researches have been done to this problem we could see that Mobile Ad hoc networks are inherently vulnerable to security attacks. While, on the other hand, it is said that the main applications of MANET are in military and emergency, all these applications are security-sensitive. MENAT can not satisfy the security requirement of the applications, so this makes that MANET is a flawed architecture.

5.2 Routing Protocol in Ad-hoc Networks

Wireless Ad-hoc Networks operates without a fixed infrastructure. Multi-hop, mobility, large network size combined with device heterogeneity and bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge. Lots of researchers did tremendous work on the Wireless Ad-hoc Routing Protocols. Two main **kinds of Routing Protocols** are existed today: one is called **table-driven protocols** (including distance vector and link state), another is **on-demand protocols**. In **table driven routing protocols**, the protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in **on-demand routing** the routes are created only when desired by the source host. While for the on demand routing protocols, "on demand "means that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources.

If we look up the key words "Wireless Ad hoc Networks Routing Protocols" in Google, we could find tons of millions of all kinds of routing protocols, as **LAR**(Location-Aided Routing), **DSDV**(Destination-Sequenced Distance-Vector Routing), **AODV** (Ad-hoc On-Demand Distance Vector Routing), and **DSR**(Dynamic Source Routing Protocol)…… .However, after survey various types of routing strategies proposed for wireless ad-hoc networks, we find the truth is all these routing protocols have inherent drawbacks and cannot be considered as good routing protocols for Wireless ad hoc Networks. Just like Windows operating systems need patch at all the time, the Wireless Ad hoc networks routing protocol are all needs patches too. The main problems about the routing protocols are as following:

1. **First** of all, consider the rapid passing pattern. We define the rapid passing pattern to be one node passing through the whole network very quickly. Such a rapid passing node will generate the following affects to the whole network. **First**, the topology of the network changed rapidly, which will lead to the lost of packets. **Second**, we have to modify every node's routing table that within the communication distance of the rapid-passing node, that will greatly improve the consumption of the bandwidth and the overhead of the networks. **Third**, obviously there will be tremendous delay of the data sending to the rapid-moving node.

2. Transmission between two hosts over a wireless network does not necessarily work equally well in both directions. Thus, some routes determined by some routing protocols may not work in some environments.

3. Many routing protocols may create redundant routes, which will greatly increase the routing updates as well as increase the whole networks overhead.
4. Periodically sending routing tables will waste network bandwidth. When the topology changes slowly, sending routing messages will greatly waste the bandwidth of Wireless Ad-hoc Networks. This will add additional burdens to the limited bandwidth of the Ad-hoc Networks.

5.3 Formal Statement of the Problem

We design a protocol that routes packets along a path which is Least Cost Path (LCP) and it does not contain malicious nodes. Also, our protocol is truthful. The setting and scenario that explained above is very well suited for analysis by means of **game theory**, more specifically by mechanism design. The purpose of a mechanism design problem is to define and explains a game. This game should be played in such a way that the outcome of the game played by independent agents according to the rules set by the mechanism designer will be the preferred outcome. This outcome is called the **social optimum**. The game should be designed based on the **dominant strategy** and results in the social optimum. The dominant means that no player has any incentive to lie and deviate from the strategy. The final state is called **dominant-strategy equilibrium** if all players playing dominant strategies in the game. The purpose of a mechanism designer is to define rules that results in dominant-strategy equilibrium.

6. Conclusion

Mobile Ad hoc Networks are an ideal technology to establish in an instant communication infrastructure less for military application or a flawed architecture has been bought out in this position paper. As we have proved using the **three main technical topics** of the Wireless Ad hoc Networks, that the Wireless Ad hoc Networks are a flawed architecture for the following technical reasons:
1. Security: The most important thing for the networks is even important for Wireless Ad hoc Networks because its applications are in military. The MANET can not appropriately solve the problem of the security.

2. Routing: is also a big problem. No suitable and stable routing protocols until now.

3. Energy consumption: problem still cannot be solved even much of efforts have been done to it.

All these prove that the Wireless Ad hoc Networks is a **flawed architectur**e. Not only because it is almost never used in practice but also because there are several technical difficulty that cannot be conquered. Besides, all the Wireless Ad-hoc Networks are expected to be self-configuration. **Self-configuration** are referring to **two aspects**, **first** construction of the network, the self-configuration network is supposed to be forming the network itself. The **other** problem is when one host moves in or moves out the Wireless Ad-hoc networks, the network should have the ability to re- configuration the topology of the whole networks. Again we could see that although many works have been done on this topic, but unlucky, all the discussions do not give us a satisfied answer to the self-configuration question. The question is never tackled in systematic way. That again prove out argument that the Wireless Ad-hoc Networks is a fundamental flawed architecture, or else we should find the appropriated answer to the problems.

However as the wireless and embedded computing technologies continue to advance, I do hope later, one day, we could build our wireless networks rely on some kinds of the Wireless Ad hoc Networks.

7. References

[1] IEEE Std. 802.11 – 1999: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications, Inst. Elec. Electron. Eng., New York, USA, 1999.ISBN 0-7381-1658-0

[2] IPN Progress Report, August 15, 2002, Analysis of Energy Consumption for Ad Hoc Wireless Sensor Networks Using a Bit-Meter-Per-Joule Metric, J.L.Gao.

[3] A Distributed Light-Weight Authentication Model for Ad-hoc Networks.

[4] M. Satyanarayanan. Fundamental challenges in mobile computing. *Submitted paper*.

[5] M. Haardt W. Mohr R. Becher, M. Dillinger. Broadband wireless access and future communication networks. *Proceedings of the IEEE*, 89(1), 2001.

[6] S.Chessa, P.Santi, "Comparison Based System-Level Fault Diagnosis in Ad-Hoc Networks", *Proc. IEEE 20th Symp. on Reliable Distributed Systems (SRDS)*,New Orleans, pp. 257-266, October 2001.

[7] Erik Skow, Jiejun Kong, Thomas Phan, Fred Cheng,Richard Guy, Rajive Bagrodia, Mario Gerla, and Songwu Lu, "A Security Architecture for Application Session Handoff".

[8] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks".

[9] David B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications,December 1994.

[10] Ljubica Blazevic, Levente Buttyan, Srdan Capkun, Silvia Giordano, Jean-Pierre, Hubaux and Jean-Yves Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes"

[11] J. A. Freebersyser and B. Leinerr, "A DoD perspective on mobile ad hoc networks," in *Ad Hoc Networking*, C. E. Perkin, Ed. Addison-Wesley, 2001, pp. 29–51.

[12] B. Leiner, R. Ruth, and A. R. Sastry, "Goals and challenges of the DARPA GloMo program," *IEEE Personal Communications*, vol. 3, no. 6, pp. 34–43, December 1996.

[14] R. Ruppe, S. Griswald, P. Walsh, and R. Martin, "Near term digital radio (NTDR) system," in *Proceedings of IEEE MILCOM*, vol. 3, November 1997, pp. 1282–1287.