Journal of Advanced Research in Cloud Computing, Virtualization and Web Applications
Volume 1, Issue 2 - 2018, Pg. No. 11-14
Peer Reviewed Journal

Research Article

# Security Measures in Cellular Aided Mobile Ad hoc Network (CAMA)

Swati Narula

Assistant Professor, Northern Institute of Engineering and Technical Campus, Alwar.

## Abstract

In this paper we present a novel infrastructure of Cellular-Aided Mobile Ad hoc Network (CAMA) with the security issues and the corresponding solutions are addressed. The experimental study shows that CAMA is much less vulnerable than a pure ad hoc network. We discuss these challenges and outline some possible solutions.

**Keywords:** Cellular Network, Wireless Security, Manets, Key Management Scheme, Ad hoc Network

## Introduction

Wireless Network is agrowing technology that allows users to access information and services electronically, regardless of their geographic position. The use of wireless communication between mobile users has become increasingly popular due to recent advancements in computer and wireless technologies. This lead to low price and high data rates, which are the two main reasons why mobile computing is expected to see increasingly widespread use and applications. Future wireless technology aims at providing an umbrella of services to its users. Ad hoc networks have become attractive for their potential for commercial applications. Routing in ad hoc network is a challenge due to the mobility of users and the lack of central control. In ad hoc networks, the issues of quality of service (QoS) and security are even more complicated because of the lack of reliable methods to distribute information in the entire network.

## System Overview

A common architecture for out-of-band signaling in support of the call-establishment, billing, routing and information exchange functions of the public switched telephone network. Another significant feature of the CAMA architecture is the availability of global information for the entire ad hoc network. A typical CAMA architecture is shown in Figure 1. It is operated in places where a mobile ad hoc network overlaps a cellular network. The routers that are in charge of working CAMA, called CAMA agents, are deployed in the cellular network. Each CAMA agent covers a number of cells and knows which mobile ad hoc user (MT) is a registered CAMA user. To get more user information, an agent should be connected with a Home Location Register (HLR). These agents collect information for the entire ad hoc network and are involved in its authentication, routing, security. Any mobile terminals may contact the CAMA agents through the cellular network's radio channels to exchange the control information. As the CAMA agent can work as a position information server, positioning routing will be applied in this architecture. This CAMA architecture can be operated in areas, which are well covered by a cellular network, such as metropolitan areas. The centralized CAMA agent is an easy solution for Authentication, Authorization and Accounting (AAA) in ad hoc networks, yet AAA is very difficult to implement in the pure ad hoc networks. Lack of AAA has been a major obstacle for commercial ad hoc networks. On the other hand, low-cost, high-data-rate ad hoc channel is suitable for wireless multimedia services. These add-on facilities over the ad hoc channel can be supplementary to the normal cellular network services. Other than peer-to-peer communications in CAMA ad hoc networks, special MTs can also act as Internet access points, through which other MTs can connect to the IP network, instead of through expensive cellular channels. The additional load of control to the cellular network is compensated by the profits generated by the integrated

**E-mail Id:** swtnarula15@gmail.com
**Orcid Id:** https://orcid.org/0000-0001-7213-9341

**How to cite this article:** Narula S. Security Measures in Cellular Aided Mobile Ad hoc Network (CAMA). *J Adv Res Cloud Comp Virtu Web Appl* 2018; 1(2): 11-14.

network. In WLAN, all the control and data packets have to go through fixed access points and only control data can goes through a cellular base station, while all other data is kept in the ad hoc network. CAMA is different from the ad hoc networks with fixed nodes (i.e., server access points), which act as base stations. In such an ad hoc network, the mobile ad hoc users might have no idea whether a fixed node has joined the network or not. The fixed nodes are difficult to access because they have the same wireless channel coverage as the mobile ad hoc users. This greatly improves ad hoc routing and security by using efficient out-of-band signaling and centralized control.

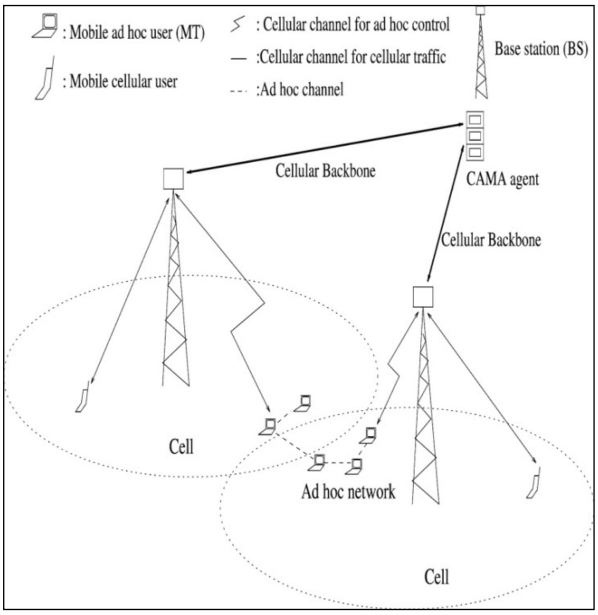

**Figure 1.Cellular-Aided Mobile ad hoc Network**

In addition, CAMA can improve the ad hoc network in:

### Synchronization

The clock for all ad hoc users cans beadjusted according to that of the cellular network in one step.

### Authentication

Any MTs can go through the same authentication procedure as in cellular networks. The mobile terminals can also be authenticated by special MTs, which can be reached easily by an entrant MT through the cellular radio channel.

### Power saving

The transmitting power of MTs can beestimated since the distance between any two MTs isWell-known. Additionally, in any new route discovery, the Intermediate MTs need not receive and forward routing packets.

### Radio resource allocation

The centralized CAMA agent can guide MTs to access the proper ad hoc channels in networks which have more than one ad hoc channel.

### Broadcasting and multi-casting

Data can be sent to the Base Station (BS) and broadcast or multicast through the cellular radio channel. No further data forwarding is needed.

### Finding cluster head in clustered ad hoc routing

In Clustered ad hoc routing, the CAMA agent can determine the cluster heads since it has the information of MTs, e.g., positions, stability and power. On the other hand, clustered routing may improve CAMA. The CAMA agent has to communicate only with cluster heads, thus reducing the load in the cellular network.

## Challenges

- We now outline the list of challenges in developing then visaged network and information infrastructure
- Dynamic topology (Movement, node failure, etc.)
- Heterogeneous and decentralized control
- Limited resources (Bandwidth, processing ability, energy)
- Unfriendly environment (Selfish nodes, malicious attackers)
- Authentication and accounting (No fixed membership)
- Security concern (Open medium without any centralized control)
- Real time services (Dynamic topology and slow routing information distribution)

## Security

Cellular networks have their own security concerns and solutions. In CAMA, our concern is for security issues related to the ad hoc network. Compared to pure ad hoc networks, achieving security in CAMA is much easier because the CAMA agent can work as a central security control point for key distributions and intrusion detections. The CAMA agent can also broadcast the information through BS whenever the network security is threatened e.g., when an intrusion is detected or a comprised MT is found. Moreover, the positioning routing is less vulnerable than other ad hoc routing protocols such as the AODV protocol. Yet CAMA has its unique security weaknesses. In cases when the GPS signals are interfered such that MTs cannot calculate their own positions, the GPS aided positioning routing will not work at all. This problem can only be solved by increasing the robustness of GPS technology. Another security weakness affecting CAMA is that the CAMA agent may be the target of attack for Denial of Service (DoS). This does not happen in pure ad hoc networks. However, the connection between the CAMA agent and an MT is very short and the number of MTs in an ad hoc network normally is not very large. Therefore, it is less likely for CAMA to suffer DoS than does the wired network.

This section discusses the security problems and the proposed solutions caused by the false position information sent by MTs, by MT's Byzantine misbehavior and by ad hocchannel jamming. It is assumed that there is no error or radio block problem in the radio channels and the malicious MTs do not collaborate with each other.

## Malicious and Selfish Nodes

Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. On the other side, selfish nodes can severely degrade network by simply not participating in the network operation.

In existing Ad Hoc routing protocols, nodes are trusted in that they do not maliciously tamper with the content of protocol messages transferred among nodes. Malicious nodes can easily perpetrate integrity attacks by simply altering protocol fields in order to subvert traffic, deny communication t legitimate nodes (denial of service) and compromise the integrity of routing computations in general. As a result the attacker can cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination increasing communication delays.

A special case of integrity attacks is spoofing whereby a malicious node impersonates a legitimate node due to the lack of authentication in the current Ad Hoc routing protocols. The main result of spoofing attacks is the misrepresentation of the network topology that possibly causes network loops or partitioning.

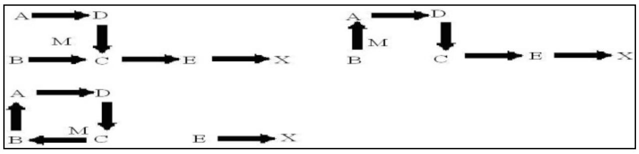

**Figure 2.Imposture in creating loop**

In figure 2, a malicious attacker M can form a routing loop so that none of the four nodes can reach the destination. To start the attack, M changes its MAC address to match A's, moves closer to B and out ofthe range of A. It then sends an RREP to B that contains a hop count to X that is less than the one sent by C, for example zero. B therefore changes its route to the destination, X, to go through A. M then changes its MAC address to match B's, moves closer to C and out of range of B and then sends to C an RREP with a hop count to X lower than what was advertised by E. C then routes to X through B. At this point a loop is formed and X is unreachable from the four nodes.

Lack of integrity and authentication in routing protocols can further be exploited through "fabrication" referring to the generation of fake routing messages. Fabrication attacks cannot be detected without strong authentication means and can cause severe problems ranging from denial of service to route subversion.

A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private connection bypassing the network. This exploit allows a node to short-circuit the normal flow of routing message creating a virtual vertex cut in the network that is controlled b the two colluding attackers.

## Security Against Byzantine Behavior

In CAMA, an MT gets to know the route from the CAMAagent and this route is carried in the header of the data packet. The MTs on the route can read the routing decision.

From the packet header, thereby knowing where the next hop is. To prevent the routing information from being changed by the intermediate malicious MTs, the information is encrypted using the source MT's secret key. The CAMA agent sends the source MT's public key to the Intermediate MTs when it pages them to wake up. The intermediate MTs can read the routing information, but cannot change it. It is possible that an intermediate compromised MT interrupts the routing information such that the MT on its next hop cannot read it. In this case, the next hop MT will report to the CAMA agent through the cellular channel. The rule for judging a malicious MT is the same as that used in detecting MTs who send the false position information.

The intermediate compromised MTs can also interrupt the Data. Watch Dog scheme can be used to avoid this attack. If the watch dog scheme is not used, the corruption of data will not be found until the destination MT tries to decrypt it. This is because data should be encrypted by a secret key only known to the source and destination MTs. Without any central control point, to find out questionable MT is difficult.

The source may have to ask every intermediate MT to senda copy of its received data packet to match with the originalone. In CAMA, with the help of CAMA agent, the bad linkcan be found more easily. There are two ways to detect such a bad link: the downlink data match and the uplink data match.

In the downlink data match, the CAMA agent broadcasts the Hash code for the original packet to all the intermediate MTs. These MTs can compare their own Hash codes with the right one. MTs then send a message confirming to the CAMA agent whether or not they received the correct data packet. This message may contain only one bit of information (0 or 1) and can be piggy-backed in some other uplink messages (e.g., the position update message). Based on the information it collects, the CAMA agent can find questionable MTs. The downlink data match method occupies less cellular radio bandwidth but does not work when there are more than one malicious MT in the route since malicious MTs may intend to send wrong messages.

In the uplink data match, the intermediate MTs send theCAMA agent the Hash codes generated from the data theyreceived and the CAMA agent makes a comparison to findout which intermediate MT received the corrupted data packet. Note that a malicious MT can only send a false message when it receives a good data packet, but it sends a wrong Hash code. It is easy to make the decision rule for the uplink data match, which is:

*From the MTs that send the right Hash code, the one closest to the destination and its next hop (this next hop MT sent awrong Hash code) are questionable and the MTs between it and the source that send wrong Hash codes are malicious.*

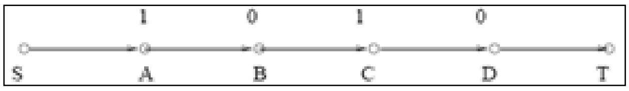

**Figure 3.Example of Hash code Comparison**

The uplink and downlink data match are compared giventhe example Hash code comparison shown in Figure 3. In Figure 3, a source S sends a data packet to the destination T through intermediate MTs A, B, C and D. T receives a corrupted data packet so a downlink data match is used. 1 is used when an MT claims that it received a good data packet and 0 is used when an MT claims it received a corrupted data packet. For the downlink match, it is difficult to make a decision since all A, B, C, D are questionable. With the uplink match, we know B is malicious and C, D are questionable. The uplink data match simplifies the judging rule, but it needs more uplink cellular bandwidth since all the intermediate MTs have to send their Hash codes to the CAMA agent separately.

## Conclusion

In this novel architecture of Cellular Aided Mobile Ad hoc Network (CAMA) a cellular network is overlaid on the ad hoc network and amobile ad hoc agent (CAMA agent) in the cellular network will manage the control signaling for the ad hoc network.

Data traffic remains in the ad hoc network. When applying the architecture, the ad hoc network performance can be greatly improved with limited cellular overhead. This architecture is also less vulnerable than a pure ad hoc network because of the availability of a central control point. The possible attacks on the architecture and the proposed solutions are addressed.

## References

1. Chakrabarti S, Mishra A. Qos issues in ad hoc wireless networks. IEEE Personal Communication Magazine. Feb 2001; 142-148.
2. Lu Y, Bhargava B. Achieving scalability and flexibility: A new architecture for wireless network. In Proceedings of Conference on Internet Computing. 2001.
3. Marti S, Giuli T, Lai K et al. Mitigating routing misbehavior in mobile wireless networks. In Proceedings of Mobico. 2000.
4. Myrick W, Zoltowski MD, Goldstein JS. Low-sample performance of reduced-rank power minimization based jammer suppression for gps. In IEEE Sixth International Symposium on Spread Spectrum Techniques& Applications (ISSSTA 2000). Aug 2000.
5. Myrick W, Zoltowski MD, Goldstein JS. Adaptive anti-jam reduced-rank space-time preprocessor algorithms for gps. In *Institute of Navigation (ION) Conference*, Sept 2000.
6. Pahlavan K, Krishnamurthy P, Hatami A et al. Handoff in hybrid mobile data networks. *I*EEE Personal Communications. Apr 2000.
7. Navstargps operation. *Web site at* http://tycho.usno.navy.mil/gpsinfo.html.
8. Albers P, Camp O, Percher JM et al. Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches. Web site at www.supelecrennes.fr/ren/perso/bjouga/ documents/.
9. Asokan N, Ginzboorg P. Key agreement in ad-hoc network. Web site at www.cs.umd.edu/ sengcy/classes/818y.

*Date of Submission:* 2018-11-21
*Date of Acceptance:* 2018-12-02