COLLISION FREE MOBILE 2 MOBILE RACH INTERACTIONS BASED ON Q-LEARNING RANDOM ACCESS

Mrs.V.Ezhilarasi[1],R.Mohamed Faisal[2],V.Panneerselvam[3],D.Prem kumar[4]
A.V.C College of Engineering& IT& Anna University& Mayiladuthurai, Tamil Nadu

[1]. Mrs.V.Ezhilarasi.,Assistant Professor ,A.V.C College Of Engineering, Mayiladuthurai.
[2]. R.Mohamed Faisal,IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
[3]. V.Panneerselvam, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.
[4]. D.Prem Kumar, IV Year, B.Tech(IT),A.V.C College Of Engineering, Mayiladuthurai.

ABSTRACT

This paper investigates the coexistence of M2M andH2H based traffic sharing the RACH of an existing cellularnetwork. Q-learning is applied to control the RACH access of theM2M devices which enables collision free access amongst theM2M user group. Frame ALOHA for a Q-learning RACH access(FA-QL-RACH) is proposed to realise a collision free RACHaccess between the H2H and M2M user groups. The schemeintroduces a separate frame for H2H and M2M to use in theRACH access. Simulation results show that applying Q-learningto realise the proposed FA-QL-RACH scheme resolves the RACHoverload problem and improves the RACH-throughput. Finallythe improved RACH-throughput performance indicates that theFA-QL-RACH scheme has eliminated the collision between theH2H andM2Muser groups.

INTRODUCTION

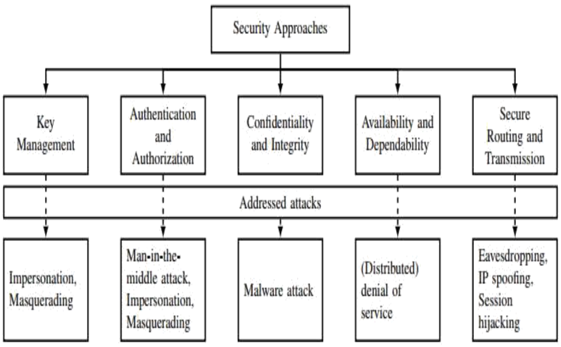
Machine-to-Machine(M2M)communication enablesdevices to communicate directly without the involvement of eNodeBs (eNBs) or the cellular core network. This improves network performance in terms of spectrum efficiency, cellular coverage, network delay, and fairness over the Long Term Evolution-Advanced (LTE-A) networks. As a result, M2M communication has been proposed to be a prospective technology to offload heavy traffic in the fifth generation (5G) where the overwhelming growth of data in cellular networks has become a critical issue

EXISTING SYSTEM:

In existing system the M2M platform to carry out the distributed computing of data transmitted from the sensors.V2X communication has been implemented in existing system

PROPOSEDSYSTEM:

- M2M enables devices to communicate directly with each other without traversing fixed network infrastructures such as access points or base stations.
- Focuses on security and privacy as two fundamental and interrelated aspects of M2M communication, which are essential for the adoption and deployment of M2M
- We provide an extensive review of latest work in M2M domain with respect to security and privacy.
- Compared with previous work on M2M security, we provide a thorough discussion dedicated to M2M privacy.
- We further derive a set of best practices and identify open problems to inspire future work on M2M security and privacy.

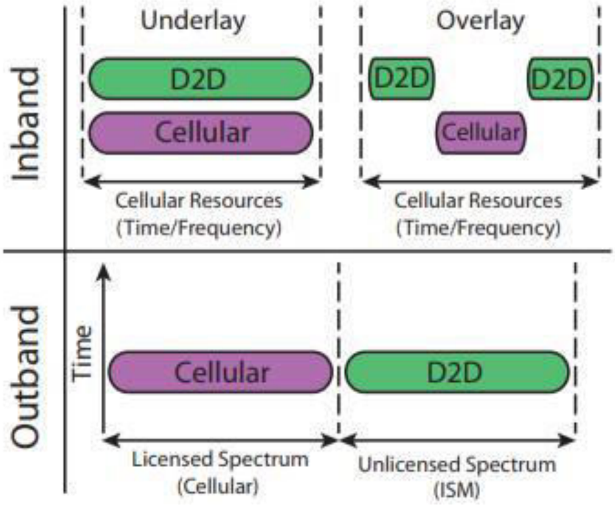

Security Approaches
Key Management
Authentication and Authorization
Confidentiality and Integrity
Availability and Dependability
Secure Routing and Transmission
Addressed attacks
Impersonation, Masquerading
Man-in-the-middle attack, Impersonation, Masquerading
Malware attack
(Distributed) denial of service
Eavesdropping, IP spoofing, Session hijacking

LITERATURE SURVEY:

Device-to-device communication is a promising technology that can offload heavy traffic in 5G networks. However, due to its open nature, there are several security issues. The LTE-A standard introduces security and protection mechanisms, which include mutual authentication between the UEs and the eNB. Unfortunately, M2M communications still face various threats: jamming, data modification, free-riding, and privacy violation. In this article, we first give architecture for an LTE-M2M system and its application scenarios with various security threats and requirements. Then we investigate privacy concerns in terms of location privacy, identity privacy, and data privacy. Afterward, we propose security solutions from aspects of application-layer security and physical-layer security, respectively. Further, we propose two frameworks for cross-application-physical-layer security methods. Finally, the challenges and future research directions are presented

M2M Communications

In the conventional cellular transmission mode, the user equipment (UE) first transmits its data to the BS using uplink resources; then the BS forwards the data to the corresponding receiver using downlink resources. However, if the transmitting UE and the receiving UE are in close proximity to each other, the BS can allow the users to directly communicate with each other. This direct transmission mode is referred to as the M2M mode .M2M communications can be integrated into cellular networks in different ways. In terms of spectrum resources, they are divided into two categories: Inband communications, in which M2M users can use the same licensed spectrum as cellular user equipments (CUEs). This category is further divided into overlay and underlay transmissions. That is, depending on the intended application, M2M communications can use dedicated resources (time/frequency), i.e., the overlay approach, or reuse the resources of other CUEs in the cell, i.e., the underlay approach. The allocation of dedicated resources is important for applications such as multi-casting and public safety, whereas resource sharing can improve efficiency of the available resources. Outband communications, in which M2M users use the unlicensed spectrum, such as the industrial, scientific, and medical (ISM) bands, for their transmissions. This, on the one hand, results in the elimination of interference to and from CUEs and, on the other hand, decreases the network control over M2Mcommunications. In addition, M2M communications need to adapt to other technologies transmitting in the same unlicensed band.


Inband
Underlay
D2D
Cellular
Cellular Resources (Time/Frequency)
Overlay
D2D
D2D
Cellular
Cellular Resources (Time/Frequency)
Outband
Time
Cellular
D2D
Licensed Spectrum (Cellular)
Unlicensed Spectrum (ISM)

A schematic view of how M2M users can access the spectrum of cellular users is illustrated. In terms of network control, M2M communications are divided into two categories: Network-assisted communications, in which the infrastructure node (i.e., the BS) assists with radio resource management, device discovery, establishing M2M connections, mobility management, and security issues. In this thesis, we will focus on network-assisted M2Mcommunications. Autonomous communications, in which, as in the Ad-hoc networks, the BS has no control over the M2M communications. The autonomous M2M communications can be used in case of network failure or when there is no coverage.

MODULES:

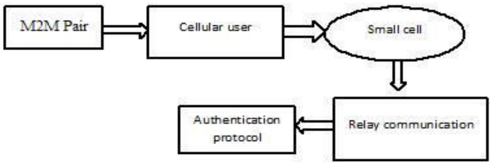
We have divided our project into small modules to improve the designing part.

- **Network design**
  - Base station model
  - Relay station model
  - Subscriber station model
- **Channel estimations**
  - Global channel estimation
    - Proactive checking
    - Passive checking
  - Limited channel estimation

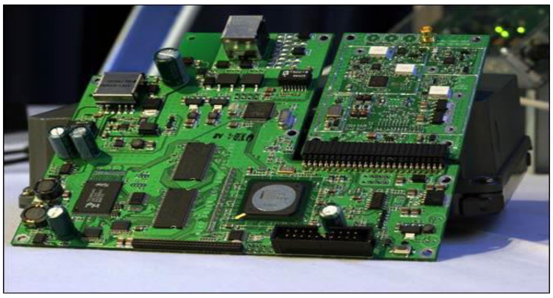
BLOCK DIAGRAM

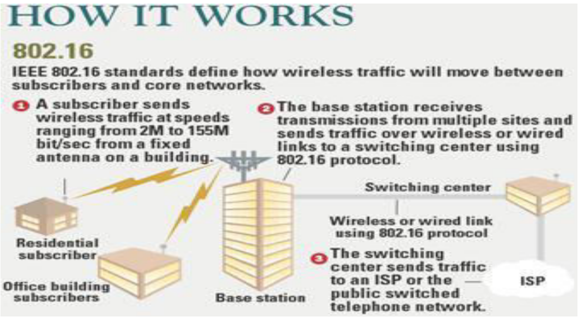
WIMAX Scenario

Consider a scenario where a WiMax-enabled computer is 10 miles away from the WiMax base station. A special encryption code is given to computer to gain access to base stationThe base station would beam data from the Internet required for computer (at speeds potentially higher than today's cable modems)The user would pay the provider monthly fee for using the service. The cost for this service could be much lower than current high-speed Internet-subscription fees because the provider never had to run cables



WIMAX CHIPS




HOW IT WORKS
802.16
IEEE 802.16 standards define how wireless traffic will move between subscribers and core networks.
1 A subscriber sends wireless traffic at speeds ranging from 2M to 155M bit/sec from a fixed antenna on a building.
2 The base station receives transmissions from multiple sites and sends traffic over wireless or wired links to a switching center using 802.16 protocol.
Switching center
Wireless or wired link using 802.16 protocol
3 The switching center sends traffic to an ISP or the public switched telephone network.
ISP
Residential subscriber
Office building subscribers
Base station

NS FEATURES

- NS is an object oriented discrete event simulator
  - – Simulator maintains list of events and executes one event after another
  - – Single thread of control: no locking or race conditions
- Back end is C++ event scheduler
  - – Protocols mostly
  - – Fast to run, more control
- Front end is OTCL
  - – Creating scenarios, extensions to C++ protocols
  - – Fast to write and change

CONCLUSION:

In this paper, we have studied security and privacy preservation issues in M2M communications underlying cellular networks. First, we have presented the system architecture of LTE-M2M systems and its applications. Then we have explained the security threats and requirements of M2M communications. Furthermore, we have investigated privacy concerns in M2M communications and propose possible solutions. Meanwhile, we have developed security solutions from the aspects of application-layer security, physical-layer security, and joint schemes, where we have proposed two frameworks for cross-physical-application-layer security. Finally, we have presented challenges and future research directions in security-aware and privacy-preserving M2M communications.

REFERENCE

[1] J. Liu et al., "Device-to-Device CommunicationsforEnhancingQuality of Experience in Software Defined Multi-Tier LTE-A Networks," IEEE Network, vol. 29, no. 4, July 2015, pp. 46–52.

[2] 3GPP, "Feasible Study for Proximity Services (ProSe)," TR 22.803, v. 12.2.0, Rel-12, June 2013.

[3] J. Due et al., "Secrecy-Based Access Control for Device-to- Device Communication Underlaying Cellular Networks," IEEE Commun. Lett., vol. 17, no. 11, 2013, pp. 2068–71.

[4] H. Zhang et al., "Radio Resource Allocation for Physical-Layer Security in M2M Underlay Communications," IEEE ICC, Sydney, Australia, June 2014.

[5] D. Zhou et al., "Device-to-Device Communications: The Physical-Layer Security Advantage," IEEE Int'l. Conf. Acoustic,Speech and Signal Processing, Florence, Italy, May 2014.

[6] Z. Hassan Awan and A. Sezgin, "Fundamental Limits of Caching in M2M Networks With Secure Delivery," IEEE ICC, London, U.K., June 2015.

[7] M. Corson et al., "Toward Proximity-Aware Internet-Working," IEEE Wireless Commun., vol. 17, no. 6, Dec. 2010, pp. 26–33.

[8] A. Acquits, L. Brandimarte, and G. Lowenstein, "Privacy and Human Behavior in the Age of Information," Science, vol. 347, no. 509, 2015, pp. 509–15.

[9] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," IEEETrans. Mobile Computing, vol. 7, no. 1, 2008, pp. 1–18.

[10] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wiretap Channel," IEEE Trans. Info. Theory, vol. 24, no. 7, 1978, pp. 451–56.