IJCSN International Journal of Computer Science and Network, Volume 4, Issue 1, February 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Review-An Approach for Data Transmission over Heterogeneous Wireless Network

[1] Sapana Nandanwar, [2] Vaishali Sahare

[1, 2] Department of Computer Science and Engineering, G.H. Raisoni Institute of Engineering & technology for Women's
Nagpur, Rashtrasant Tukadoji Maharaj University
Nagpur, Maharashtra, India.

Abstract - Machine to Machine Communication (M2M) is the automatic exchange of data in a heterogeneous wireless network, including devices or machines, without human interaction. MTC applications aim to provide quality to the machine with, in order to automated every life process. MTC devices are generally spread in a various area and should communicate with each other in various networks. LTE cellular networks are decide to support MTC applications then its offer a large coverage and these are all heterogeneous networks. The advantage of such method is for both MTC application and LTE networks. The most necessary of these problems is the congestion in network which is form However; the MTC applications over LTE networks occur many requirements and causes challenges due to congestion in network. In propose design, long term evolution use heterogeneous network and according to particular network, security will be provided. The security of wireless sensor networks is a challenging problem in the process of data transmission.

Keywords - *Machine to Machine Communication, Heterogeneous Network, Wormhole Attack, Security.*

1. Introduction

Heterogeneous Wireless Network is defined as a special case of heterogeneous network whereas a heterogeneous network consists of a network of computers or device. Heterogeneous Wireless Sensor Networks (HWSNs), where sensor nodes have different capabilities in terms of communication, computation, energy supply, storage space, reliability and communication overhead in network. Consider an HWSN consisting of two types of wireless sensors: a small number of high-end sensors (H-sensors) and a large number of low-end sensors (L-sensors). Security is critical to wireless sensor networks deployed in hostile environments, such as military battlefield and security monitoring as well as digital signature [2]. Key Pairing is an essential cryptographic primitive upon which other security primitives are built in network [2]. In heterogeneous wireless network, use one method i.e. Long term evolution (LTE) and it is standard use for the wireless data communication, evolution of various standard like GSM/UMTS. To provide data transmission in M2M communications will be small in size, but high in frequency. M2M devices will be mostly inactive, when number of packets in buffer is zero and become active only when there is a need for data transmission and also when number of packets is more than threshold.M2M devices and H2H users can coexist in the same network such as the emerging long-term evolution (LTE).

LTE networks mainly use a frequency reuse of to maximize use of the licensed bandwidth. In heterogeneous networks, the cells of different sizes are referred to as macro-cell, micro-cell, Pico-cell and femtocells; listed in order of decreasing base station power. Long-Term Evolution (LTE) allows operators to use new and old spectrum and complements 3G networks with higher data rates, lower latency and a thick, IP-based architecture [1]. Some packets can be corrupted due to the congestion in network. So use a Wormhole attack in a heterogeneous network. A Wormhole attack is composed of two attackers and a Wormhole tunnel.

To establish a Wormhole attack, attackers create a direct link, referred to as a Wormhole tunnel, between them. The wormhole tunnel can be established by means of a wired link, a high quality wireless out of band links, or a logical link via packet encapsulation. In a wormhole attack using a wired link or a high quality wireless out of band link, attackers are directly linked to each other, so they can communicate swiftly [5]. To overcome such challenges, many security primitives are required such as data authentication, unforgeability, non repudiation, and confidentiality of message contents; however these primitives require the usage of keys using key management [2].

2. Related Work

Ping Wang, Dong in Kim [1], present a unified performance modeling and analysis framework for the heterogeneous MTC devices. These devices may have different settings (e.g., packet generation rate) and can work in different scenarios.

The performance modeling and analysis is composed of the following components:-

i) Introduce a tractable queuing model for MTC UEs with random access to initiate connections for transmitting data to the MTC User. The queueing model enables us to analyze the data transmission performance of heterogeneous MTC UEs with the energy saving capability. That is, the MTC UE can switch to an inactive mode to reduce its energy consumption when its buffer is empty.

ii) It presents the coalitional game model for eNodeB selection and coalition formation for relay transmission. Consider the small cell network environment, where a macro cell is under laid by small cells (e.g., femtocells).In addition; MTCUEs can form data or packets and perform relay transmission to reduce congestion in the network.

iii) He have presented the optimization and analysis of the machine-to-machine (M2M) or machine-type-communications (MTC) coexisting with the human-to-human (H2H) communications in long-term evolution (LTE) networks. Specifically, have presented the analytical queueing model to obtain the performance measures of MTC UEs, which can opportunistically obtain preambles for their Connection initialization when H2H UEs do not occupy the preambles.

K. Naga Divya, K.Sri Vijaya [2], proposed an Efficient ECC based Key management scheme against non-differential side channel attack has been presented and also represent authenticates the data and then exchange of key. This scheme reduces storage space Requirement, Communication overhead in network and provides security using Elliptic Curve Cryptography. This approach also ensures keep safe of energy consumption for point multiplication, if number of doubling operations is more than three times to that of addition operations in point multiplication. If one node is compromised in network, then the probability of compromising other node with captured information is zero since the keys are independent to each node. This can be extended by applying to all types of elliptic curves with some modification. M.-Y. Cheng, G.-Y. Lin, H.-Y. Wei, A. C.-C. Hsu [3], to conduct and represent comprehensive study to different RAN-overload resolution methods, a comparison between the performances of different mechanisms is also provided. It conclude that RAN/CN resources are insufficient to meet the needs of all users and MTC devices, and the promising solution is to discriminate UE/MTC devices, protect H2H traffic from server service degradation, and reduce signaling overload from MTC devices.

Shao-Yu Lien and Kwang-Cheng Chen [4], It provide an overview of M2M communications in 3GPP, with a particular focus on the air interface, including the physical layer transmission schemes, random access procedure, and radio resource management for QoS guarantees, to fully comprehend practical issues of enabling M2M communications over LTE-Advanced. It provide an overview of M2M communications in 3GPP, with a particular focus on the air interface, including the physical layer transmission schemes, random access procedure, and radio resource management for QoS guarantees, to fully comprehend practical issues of enabling M2M communications over LTE-Advanced. The provided elaborations show that the characteristics of M2M communications are very different from those of H2H communications.

Husain Shahnawaz, Joshi R.C [5], propose Wormhole attack is applied in the adhoc wireless network using reactive routing protocol AODV. This propose for Worm-Hole attack is assume in the network, statistics are decide to design intrusion detection engine for MANET. Necessary features extraction and rule inductions are use to applied to classify the data set. Wormhole attack is a severe attack in wireless network and it records the packets.

Dr. Esam A. A. A. Hagras, Doaa El-Saied, Dr. Hazem H. Aly [6], propose an efficient Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks (HWSN).It use elliptic curves for their high security and small key size. In addition, the new method achieves forward secrecy, integrity and encrypted message authentication. The scheme's forward secrecy property ensures that past messages remain confidential even if the sender's private key is compromised in network. Public verifiability enables any trusted/un-trusted judge when dispute occurs to verify the signature of original message

without revealing any secret information. Also, the performance evaluation shows that this key management can achieve significant reduction in storage space compared with other previous methods.

3. Proposed Design

In proposed design, dividing into three parts is as follows: A) Machine to Machine communication and B) Elliptic curve cryptography C) Wormhole attack.

3.1. Machine to Machine Communication

The system proposed is able to perform the data transmission over heterogeneous wireless network. In heterogeneous wireless network, base station, MTC user (LTE) etc. are required. Machine to Machine communication comprises a wireless network where base station sends the data or information to MTC user about what they are doing. Consider one microcell in heterogeneous network with one base station. Dividing into two parts:-i) Machine to machine communication and ii) Human to Human communication.

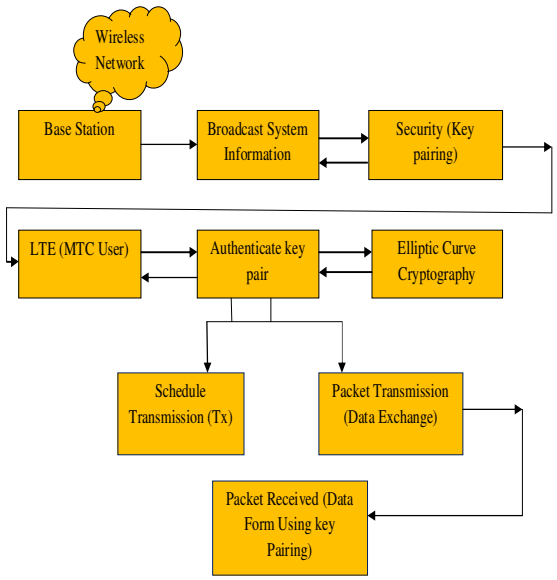

Fig. 1 An Approach for Data Transmission Over Heterogeneous Wireless Network

From the figure 1, Base station can transmit the system broadcast information to the LTE (MTC User) and then provide a security like key paring. Authenticate the data and exchange of key to encrypt the packets. Some Packets is loss due to congestion in network then use Wormhole Attack. In that, Attacker records the packets at one location to another location and retransmits the packets to another using Elliptic Curve Cryptography. This elliptic curve cryptography can authenticate the data properly. These packets can be transmitting using schedule transmission in time or sec and then the packet is received.

3.2. Elliptic Curve Cryptography

Elliptic Curve cryptography (ECC) takes limited power consumption for Wireless Sensor network. One main advantage of ECC is having small size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA. Most existing key management methods try to established keys for all pairs of sensors, whether these nodes communicate with each other or not in network, and this causes large overhead in heterogeneous network. This scheme provides significant reduction in communication overhead, storage space and power consumption, integrity than another key management scheme. These support the creation of key and then authenticate, encrypt the particular data or information and so on. This algorithm is mainly based on the algebraic structure of elliptic curves. The difficulty in problem is the size of the elliptic curve.

3.3. Wormhole Attack

For the proposed design, use the wormhole attack. This is one type of a passive attack. This attack prevent some packets are properly sent to the MTC user in heterogeneous network. Wormhole attack is severe attack in wireless network. In that attack, attacker has not compromise any hosts and all communication provides authenticity, integrity and so on. In this attack, attacker can records the packets at one location to another location in the wireless network and retransmits packet to the other network. For example, most existing adhoc wireless network without some mechanism to defend against the wormhole attack would be unable to find the routes no longer than two hops with disrupting communication.

Table 1.Comparsion of Algorithm

Parameters	**Algorithms**	
	Uniform Back-off Algorithm[1]	**Iterative Algorithm[4]**
Network Overhead	Less	Less
Throughput	More	More
Packet loss	Less	Less
Success Rate	More	More

4. Conclusion

This paper proposes an approach for data transmission over Heterogeneous wireless network to send a data in particular manner for packet transmission. The system proposed in this paper is able to perform the data transmission in heterogeneous wireless network especially reducing, or completely avoiding congestion issue induced by a considerable number of devices, trying to connect to the network, or send data. This is precisely emphasized in this report. In fact, one of the most important and active research orientations of mobile cellular networks is to get all possible efficient techniques to meet the requirements of M2M applications, so as to take advantages of their benefits, especially the growth market of M2M communications.

References

[1] Ping Wang, Dong In Kim, "Performance Modeling and Analysis of Heterogeneous Machine Type Communications", IEEE Transactions on Wireless Communications., vol .13,no 5,pp. 2836-2849, May 2014

[2] K. Naga Divya, K.Sri Vijaya, "A Routing- Driven Elliptic Curve Cryptography based key management scheme for heterogeneous sensor networks" , IEEE Journal on Computer Science and Software Engineering, vol.2, no 9,pp.442-449,September 2012

[3] M.-Y. Cheng, G.-Y. Lin, H.-Y. Wei, A. C.-C. Hsu, "Overload control for machine-type-communications in LTE-Advanced system," IEEE Commun. Mag., vol. 50, no. 6, pp. 38-45, June 2012.

[4] S.-Y. Lien, K.-C. Chen, and Y. Lin, "Toward ubiquitous massive accesses in 3GPP machine-to-machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 66-74, Apr. 2011 .

[5] Husain Shahnawaz, Joshi R.C, "Design of Detection Engine for Wormhole Attack in Adhoc Network Environment", Inter-national Journal of Engineering and Technology (IJET), vol4, no 6,pp. 381-395, Jan 2013.

[6] Dr. Esam A. A. A. Hagras, Doaa El-Saied, Dr. Hazem H. Aly"A New Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wire- less Sensor Networks",IJSCT,vol 2,issue 2,pp. 19-23,June2011

Authors

Sapana Nandanwar Pursuing M.E 4th sem from G.H. Raisoni college of Engineering and Technology for Women Nagpur**,** Maharashtra, India.Her research interests are in the area of the Wireless Sensor Network.

.

.

.