International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 1
ISSN: 2454-4248
164 - 168

Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks

Mrs.C.Sathya.,M.Sc [1], Mrs.T.Vijaya saratha.,M.sc,M.Phil[2], Mrs.K.K.Kavitha, M.C.A,M.Phil,.SET.,(Ph.D)[3]
Research Scholar, Dept. of Computer Science, Selvamm Arts & Science College (Autonomous), Tamilnadu, India [1]
Asst.Professor, Dept. of Computer Science, Selvamm Arts & Science College (Autonomous), Tamilnadu, India [2]
HOD, Dept. of Computer Science, Selvamm Arts & Science College (Autonomous), Tamilnadu, India[3]

Abstract::- Internet of Things is increasing the network by group action immense quantity of close objects which needs the secure and reliable transmission of the high volume knowledge generation, and also the mobile relay technique is one among the economical ways in which to satisfy the on-board knowledge explosion in LTE-Advanced (LTE-A) networks. However, the observe of the mobile relay can cause potential threats to the knowledge security throughout the relinquishing method. Therefore, to handle this challenge, during this paper, we have a tendency to propose a secure relinquishing session key management theme via mobile relay in LTE-A networks. Specifically, within the planned theme, to realize forward and backward key separations, the session key shared between the on-board user instrumentality (UE) and also the connected donor evolved node B (DeNB) is initial generated by the on-board UE then firmly distributed to the DeNB. moreover, to cut back the communication overhead and also the process complexness, a unique proxy re-encryption technique is used, wherever the session keys at the start encrypted with the general public key of the quality management entity (MME) are going to be re-encrypted by a mobile relay node (MRN), so alternative DeNB will later rewrite the session keys with their own non-public keys whereas while not the direct involvement of the MME. elaborated security analysis shows that the planned theme will with success establish session keys between the on-board UEs and their connected DeNB, achieving backward and forward key separations, and resisting against the collusion between the MRN and also the DeNB because the same time. Additionally, performance evaluations via in depth simulations area unit applied to demonstrate the potency and effectiveness of the planned theme.

Keyword: *Handover, Mobile communication, Internet of things, Relays, Security, Mobile computing.*

*****

1. INTRODUCTION

The Third Generation Partnership Project (3GPP) has identified machine type communication(MTC) to be one of the facilitators for IoT in LTE-Advanced(LTE-A) networks, and the highly penetrated portable electronic devices (smart phones, tablets, etc.) are regarded as common contact points or gateways for the large-scale deployment of IoT devices Advanced transportation(high-speed trains, buses, trams, cars, etc.) which are moving along the rails/roads and equipped with various sensors a enough processing power, are perfect candidates for the real-time environmental monitoring and mapping, which is an indispensable part of IoT For the information and data collected by the on-board sensors, they can be aggregated and processed by the on-board units, and then transmitted to the Internet by on-board mobile devices.

In the meanwhile, the mobile devices which belong to the passengers are also responsible for managing the small scale autonomous networks, and the constant wireless broadband network access is mandatory for these on-board mobile devices However, for public transportation, due to the fast moving well-shielded carriage, data transmission will suffer from high penetration path loss, severe Doppler frequency shift, and low handover success rate caused by a large number of on-board mobile devices performing frequent handovers simultaneously.

To circumvent the above problems, the concept of mobile relay is proposed in the 3GPP in LTE-A networks A mobile relay consists of an outer antenna mounted on the top of the moving transportation providing a wireless backhaul with a Donor evolved Node B (DeNB) located along the roadside, while the wireless connection to the on-board users is realized by the inner antenna installed inside the carriage LTE is a wireless broadband technology designed to support roaming on cell phones and handheld devices.

LTE offers significant improvements over previous cellular communication standards. OFDM used in LTE systems make it possible to supply high-speed data service on railway But there are still many problems to be solved. In wireless systems for high speed rail, BS are deployed in a straight line along the rail and handover happens in the overlapped areas, whose performance, including handover probability, handover delay and unnecessary handover number caused by Ping-Pong effect will be degraded seriously. However, there are many problems still remain unsolved for the handover in wireless communications for high speed rail, such as the handover triggered probability, which is the probability of handover triggered before the

 ISSN: 2454-4248
164 - 168

train arrives at a specific position A higher handover triggered probability is desirable at the cell edge to avoid communication interruptions and call drops to ensure continuous communication.

2. RELATED WORK

I used the EURANE module and a LTE queue development package in the ns-2 simulator to implement the EPS security framework—which includes EPS-AKA, the inter-eNodeB handover described in the KDF operation, we manually added the processing delay that is part of the EPS-AKA by using Hash-based Message Authentication Code (HMAC) with the Secure Hash Algorithm (SHA)-256 as measured by a Polar SSL on an Intel Pentium IV 3.0 GHz with 1 GB of random-access memory. The average operation speed and standard deviation for HMAC-SHA-256 are 16.635 and 0.081 microseconds, respectively. A source eNodeB and the MME require one HMAC-SHA-256 operation each to calculate a new KeNB and an NH value, respectively. The UE needs to synchronize NCC values by performing HMAC-SHA-256 operations equal to the number of horizontal handovers and computes the current NH value once. The length of all key materials is defined as 128 bits except that KeNB and NH are 256 bits.

SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2), and is one of the strongest hash functions available. While SHA-1 has not been compromised in real-world conditions, SHA-256 is not much more complex to code, and has not yet been compromised in any way. The 256-bit key makes it a good partner-function for AES. It is defined in the NIST (National Institute of Standards and Technology) standard 'FIPS 180-2'. NIST also provide a number of test vectors to verify correctness of implementation. In this script as clear and concise as possible, and equally as close as possible to the NIST specification, to make the operation of the script readily understandable.

3. EXISTING SYSTEM

Existing analyzes the authentication and key agreement protocol adopted by Universal Mobile Telecommunication System (UMTS), an emerging standard for third-generation (3G) wireless communications. The protocol, known as 3GPP AKA, is based on the security framework in GSM and provides significant enhancement to address and correct real and perceived weaknesses in GSM and other wireless communication systems. 3GPP AKA protocol is vulnerable to a variant of the so-called false base station attack. The vulnerability allows an adversary to redirect user traffic from one network to another. It also allows an adversary to use authentication vectors corrupted from one network to impersonate all other networks. Moreover, we demonstrate that the use of synchronization between a mobile station and its home network incurs considerable difficulty for the normal operation of 3GPP AKA. Security problems in the 3GPP AKA, we then present a new authentication and key agreement protocol which defeats redirection attack and drastically lowers the impact of network corruption. The protocol, called AP-AKA, also eliminates the need of synchronization between a mobile station and its home network. AP-AKA specifies a sequence of multiple flows.

3.1 Disadvantages of Existing System:

- Security is a vital issue in existing.
- The base station attack reduces the networking lifetime.
- The user traffic can be occurred while the authentication process.

4. PROPOSED SYSTEM

Security has become the main concern and bottleneck for widely deployed wireless applications. This issue can be seen in two aspects: First, the open shared access medium is vulnerable to attacks. Second, the wireless resources are stringently constrained. The spam attack, which is a kind of flooding Denial of Service (DoS) attack, can be carried out by the anti-node inside the sensor network. Such attack can retard the message transmission and exhaust the energy of a sensor node by generating spam messages frequently. In previous cases, the authors propose detect and defend spam (DADS) scheme and quarantine region scheme (QRS) to address the following issues: spam detection, quarantined nodes determination, messages authentication, and quarantine region cancelation. Two detection mechanisms against spam attacks on sensor networks are proposed in DADS. The first method is to filter incoming messages according to their contents and detect the nodes that send faulty messages frequently. The second method uses the frequencies of messages sent by the sensors in the same region. In DADS, the anti-node is detected by the sink, not by the sensor node. The packets of each sensor are counted by the sink. Such centralized detection architecture can be well suitable to a small-scale sensor network, but the total number of packets could be large in a large-scale sensor network.

4.1 Benefits of Projected System:

- The proposed algorithm results high throughput.
- The proposed system provides secure and reliable transmission.

 ISSN: 2454-4248
164 - 168

5. IMPLEMENTATION

Anti-node detection

In order to strengthen the network against spam attacks, the secure control is embedded into the SADTCA. An authenticated broadcasting mechanism, such as the μ TESLA in SPINS, may be applied in this phase. In the authenticated broadcasting mechanism, a challenge is made for all sensors in the field such that normal nodes and anti-nodes can be differentiated. The challenge is that when a sensor broadcasts a Hello message to identify its neighbors, it encrypts the plaintext and then broadcasts; when receiving the Hello message, the sensor decrypts it. If the sensor decrypts the received message successfully, the sender is considered normal. Otherwise, the sender is said to be an anti-node. Therefore a network topology is formed without anti-nodes in order to make the network safe.

Cluster head selection

Each sensor sets a random waiting timer, broadcasts its presence via a 'Hello' signal, and listens for its neighbor's 'Hello.' The sensors that hear many neighbors are good candidates for initiating new clusters; those with few neighbors should choose to wait. By adjusting randomized waiting timers, the sensors can coordinate themselves into sensible clusters, which can then be used as a basis for further communication and data processing.

Gateway selection

Observe that the clustering scheme induces non-overlapping clusters. Accordingly, to interconnect two adjacent non-overlapping clusters, one cluster member from each cluster must become a gateway. This subsection presents a method of choosing distributed gateways for adjacent non-overlapping clusters. Random waiting times and local information are applied to select gateways and further achieve communication between clusters.

Key distribution

According to the cluster construction in cluster formation, a simple and efficient key distribution scheme is applied in the network. In this phase, two symmetric shared keys, a cluster key and a gateway key, are encrypted by the pre-distributed key and are distributed locally. A cluster key is a key shared by a cluster head and all its cluster members, which is mainly used for securing locally broadcast messages, e.g., routing control information, or securing sensor messages.

Key renewal

Initially all cluster heads (CHs) choose an originator to start the "key renewals", and then it will send the index to all cluster heads in the network. There are many possible approaches for determining the originator. For instance, the cluster head with the highest energy level or the cluster head with the lowest cluster ID. After selecting the originator, it initializes the "Key renewal" process and sends the index to its neighboring clusters by gateways. Then the cluster head refreshes the two keys from the key pool and broadcasts the two new keys to their cluster members locally. The operation repeats the way through to all clusters in the network

5. PERFORMANCE AND EVALUATION

The proposed algorithm results high throughput due to clustering and dropping un authentication packet. Comparing to the existing scheme JATC and LLISE, the proposed Secure Adaptive Distributed Topology Control Algorithm have high throughput and it defend the spam attack as per simulation outcome.

Fig: 6.1 Comparison of Throughput vs. Number of iteration

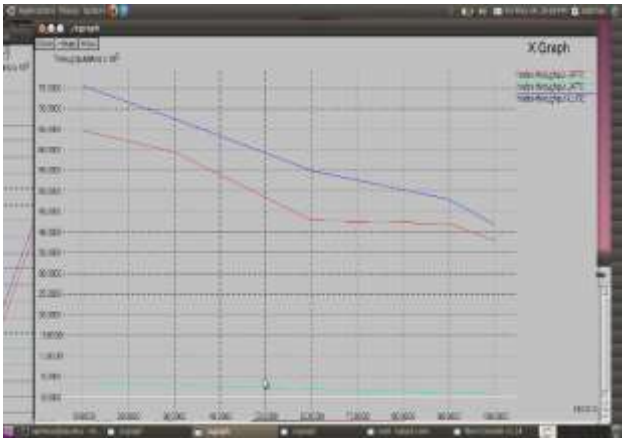

Fig: 6.2 Graph evaluation of throughput

 ISSN: 2454-4248
164 - 168

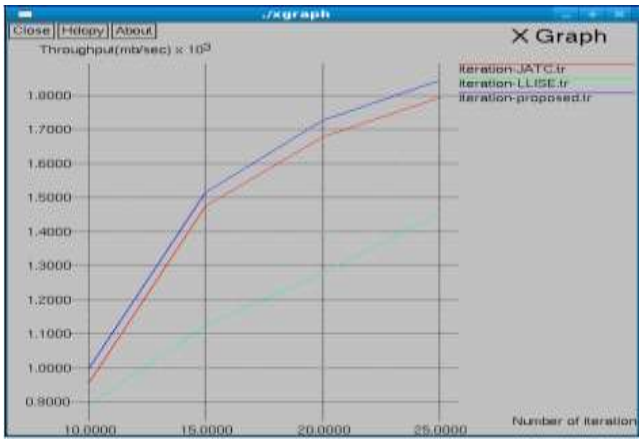

Fig: 6.3 Comparison of existing system and proposed system

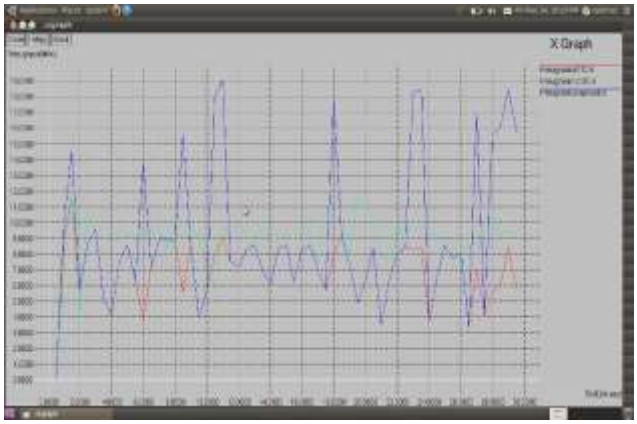

Fig: 6.4 Throughput comparison existing system and proposed system

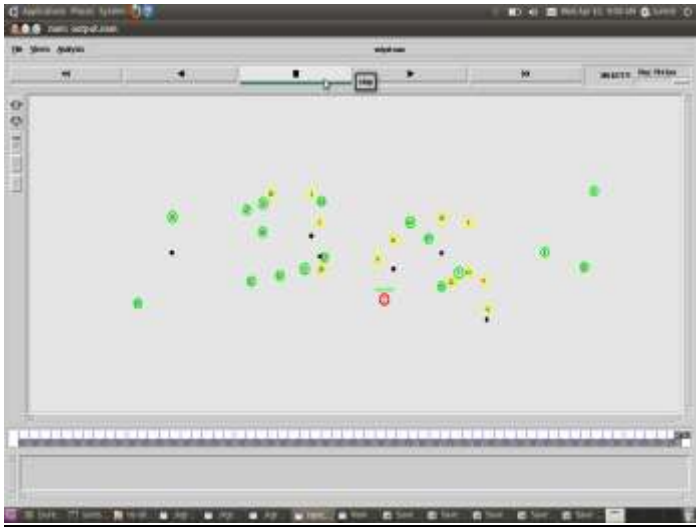

Fig: 6.5 Node movements in nam output window

6. CONCLUSION

In this thesis I have deliver a review of LTE handover key management security procedure and I was concerned with the threats on forward key separation in handover key management, and how to describe the packets exposed to de synchronization attack using different distribution functions to select an optimal handover key update interval that helps network operators to enhance the detection and prevention techniques. Using the lognormal distributions model is more suitable for fitting the residence time distribution than in the gamma model and it provides a good approximation to be beneficial when modeling packet loss with key update interval. Although periodically updating the root key minimizes the effect of the attacks from selecting an optimal key update interval is an ill-defined problem because of the difficulty of achieving a balance between the signaling load and volume of exposed packet. I have derived a mathematical structure for selecting a best possible handover input update interval that helps a network operator select a best rate that fits best with system organization policies.

FUTURE WORK

In the future work, I have plan to involve more mechanisms to make the protocol faultless and practical, such as developing a new algorithm to identify anti-network sensors and proposing efficient security mechanisms to make protocol suitable for adaptive topology management.

REFERENCES:

[1] "3GPP System Architecture Evolution (SAE); Security Architecture (Release 11)," 3GPP TS 33.401, Version 11.2.0, Dec. 2011.

[2] "3G Security, Security Architecture (Release 8)," 3GPP TS 33.102, Version 11.1.0, Dec. 2011.

[3] M. Zhang et al., "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Comm., vol. 4, no. 2, pp. 734-742, Mar. 2005.

[4] C.B. Sankaran, "Network Access Security in Next-Generation 3GPP Systems: A Tutorial," IEEE Comm. Magazine, vol. 47, no. 2, pp. 84-91, Feb. 2009.

[5] V. Niemi et al., "3GPP Security Hot Topics: LTE/SAE and Home (e)NB," Proc. ETSI Security Workshop, Jan. 2009.

[6] Y. Park et al., "A Survey of Security Threats on 4G Networks," Proc. IEEE GlobeCom Workshop Security and Privacy in 4G Networks, Nov. 2007.

[7] I. Bilogrevic et al., "Security and Privacy in Next Generation Mobile Networks: LTE and Femtocells," Proc. Int'l Femtocell Workshop, June 2010.

[8] O. Altrad and S. Muhaidat, "Intra-frequency handover algorithm design in LTE networks using doppler frequency estimation," in Workshops Proceedings of the Global Communications Conference, GLOBECOM2012, 3-7 December 2012, Anaheim, California, USA, 2012, pp. 1172–1177.

ISSN: 2454-4248
164 - 168

[9] Y. Sui, J. Vihri¨al¨a, A. Papadogiannis, M. Sternad, W. Yang, and T. Svensson, "Moving cells: a promising solution to boost performance for vehicular users, "IEEE Communications Magazine, vol. 51, no. 6,2013.

[10] N. Lin, X. Huang, and X. Ma, "Analysis of the uplink capacity in the high-speed train wireless communication with full-duplex mobilerelay," in IEEE 83rd Vehicular Technology Conference, VTC Spring2016, Nanjing, China, May 15-18, 2016, 2016, pp. 1–5.

[11] F. Y. Lin, C. Hsiao, K. Chu, and Y. Liu, "Minimum-cost qos-constrained deployment and routing policies for wireless relay networks, "J. Applied Mathematics, vol. 2013, pp. 517 846:1–517 846:19, 2013.

[12] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3gpp and wimax networks," in IEEE International Conference on Communications, ICC 2014, Sydney, Australia, June 10-14, 2014,2014, pp. 1011–1016.

[13] G. M. Køien, "Mutual entity authentication for LTE," in Proceedings of the 7th International Wireless Communications and Mobile Computing Conference, IWCMC 2011, Istanbul, Turkey, 4-8 July, 2011, 2011, pp.689–694.

[14] D. Forsberg, "LTE key management analysis with session keys context," Computer Communications, vol. 33, no. 16, pp. 1907–1915, 2010.

[15] "3GPP system architecture evolution (SAE); security architecture (Re-lease 11),"3GPP TS 33.401, 2011.