ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

National Symposium On Emerging Trends In Computing & Informatics, NSETCI 2016, 12th July 2016, Rajagiri School of Engineering & Technology, Cochin, India

An Encoded Key Management Scheme for Wireless Multicast Networks.

***Saranya.M.S[1] and Prof. Vigil Kumar.V.V[2].**

1. M.Tech Network Engineering, Department of IT,GEC Idukki.
2. Assistant Professor and HOD, Department of IT, GEC Idukki.

Manuscript Info

Key words:
Group key management, mobile multicast, security,backward confidentiality

Abstract

Key management in mobile multicast communication generally involves variety of issues due to the convergence of wireless and mobile technologies. Users could subscribe to the services while they are ubiquitous. However, the existing group key management (GKM) protocols intend to secure group communication for just a single group service. The GKM approaches involve inefficient use of keys and communication overheads, hence unsuitable for multiple multicast group environment. A novel GKM protocol for multiple multicast groups, called slot based multiple group key management (SMGKM) scheme using encoding is being proposed. SMGKM supports the movement of single and multiple members across a homogeneous or heterogeneous wireless network while participating in multiple group services with minimized communication overheads. Unlike conventional GKM protocols, SMGKM protocol can mitigate one- affect-n phenomenon, single point of failure and investment pressure of signalling load caused by rekeying at the core network. To provide backward confidentiality, a 256 bit hash encoding technique is used when rekeying is done as users move from one cluster to another.Analysis of results shows that the communication overhead incurred is less in SMGKM scheme while packet delivery ratio and throughput are high in SMGKM scheme compared to conventional schemes

Introduction:-

Emerging mobile wireless applications depend on secure group communications. Key is made secure using various cryptographic or hash algorithms and group key is changed whenever a member joins or leaves the group session. This is done to ensure backward confidentiality so that the future messages cannot be retrieved by the departing member of that group. Group Key Management Protocols generallydeals with the distribution, updation and revocation of Keys. Mobility often complicates the key management by allowing not only join or leave the group which requires rekeying but also to change the areas. Multicast is an efficient communication technology for the provision of group oriented services over the Internet. These include services such as VOD (Video on Demand) and video conferencing. The services could be deployed more comfortably in wireless mobile networks than in wired networks because the entire receiving nodes within the transmission range of the broadcast medium can receive the services in a single transmission. Thus, the multicast services are expected to be dominating services by considering the fact that the majority of the recent standards committees of wireless networks such as E-MBMS in LTE (G.S.Rao, 2008)have standardised them. With the emergence of diverse group-based services, multiple multicast groups are likely to coexist in a single network, and users may subscribe to multiple groups simultaneously. However, the existing group key management (GKM) schemes, aiming to securecommunication within a single

group, are not suitable in multiple multicast group environments because of inefficient use of keys, and much larger rekeying overheads. In this paper, a new scheme called slot based multiple group key management (SMGKM) scheme.SMGKM supports the movement of single andmultiple members across a homogeneous or heterogeneous wireless network while participating in multiple group services with minimized rekeying transmission overheads. Unlike conventional GKM protocols,SMGKM protocol can mitigate one-affect-n phenomenon, single point of failure and investment pressure of signalling load caused by rekeying at the core network.

A. Wireless Multicast Networks:-

Multicast (G.S.Rao, 2008) (3GPP,2007) is the delivery of a message or information to a group of destination computers simultaneously in a single transmission. Such applications need a secure group key to communicate their data. This brings importance to key distribution techniques.The advantage of multicast is that, it enables the desired applications to service many users without overloading a network and resources in the server. In multicast group communication, all the authorized members share a session key, which will be changed dynamically to ensure backward confidentiality referred as group rekeying. Since the wireless networks are vulnerable to various security attacks therefore there is a need for access controlmechanisms.

Consequently, it is predictable that in the future, multiple multicast groups will co -exist within the same network due to the emergence of various group-based applications and computationally fast mobile devices along with increased data rates or next generation wireless networks. Such a situation is probable to cause substantial key management overhead at the service provider (SP) for supporting multigroup services. Thus, the existing GKM schemes for secure wired and wireless mobile multicast networks will suffer from rekeying performance for cumulative multicast services because there are only targeted for a single multicast service.

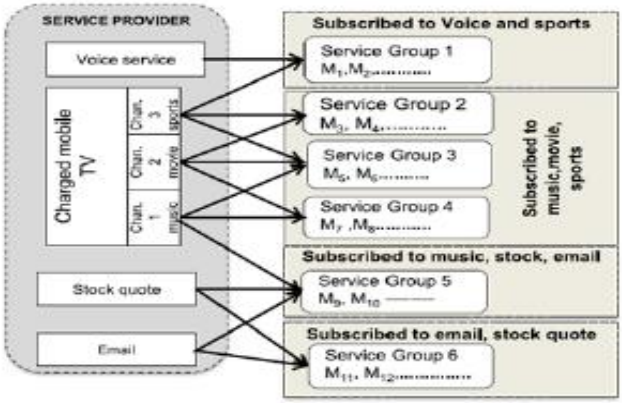

Figure i Multiple Services. [1]

B. Rekeying Multicast Group:-

To solve the rekeying complexity as multicast services cumulate in a single network,anovel slot based multiple group key management (SMGKM)protocol is proposed for managing both single-move and multi-moves across a wireless network while seamlessly participating in multiservices with minimized rekeying transmission overheads, reduced communication and storage overheads, no singlepoint of failures, no one- affect-n phenomenon and optimized signalling load at the core network. In SMGKM the key management tasks is offloaded to the intermediate cluster managers called Area Key Distributors (AKD) which establish the necessary key management keys. SMGKM integrate our concept of session key distribution list (SKDL) introduced for fast and secure authenticated handover alongwith initial key establishment. SMGKM employ a lighter symmetric encryption suitable for resource constraint mobile devices than heavier asymmetric effort. Compared to the existing schemes, SMKGM save enormous communication bandwidth utilization in the presence of multi-handoffs inmulti services. The new concept offers the following benefits over the previously proposed schemes:

- Move the authentication of individual mobile receivers from the DKD to the area intermediate trusted key distributor AKD. This alleviates unnecessary delays and possible bottlenecks at the DKDin large distributed multicast network involving several services.

- Reduce the rekeying traffic between the AKDs and DKDs which is replaced by the traffic to the SP,which needs to be notified of each rekeying
- Allow the intermediate trusted AKDs to establish and securely distribute the service encryption keys for affected services due to host mobility/handoff. This is done in a scalable manner without involving the trusted DKD. In fact rekeying is handled locally to alleviate 1- affect-n phenomenon and reduce communication overheads.

Related Works:-

(Sandro Rafaeli.et.al, 2003) took a survey of traditional GKM protocols addressing rekeying over wired networks.Protocols are divided in to centralized, decentralized and contributory schemes. The three classes are described in the paper and an insight given to their features and goals.In centralizedarchitecture, the group key management protocol (GKMP) enables the creation and maintenance of a group key.In the decentralized subgroup approach,the large group is split into small subgroups. Different controllers are used to manage each subgroup, minimizing the problem of concentratingthe work on a single place.

(Mohammed Riyadh.et.al, 2015) says that constrained devices in the Internet of Things (IoT) will often operate in groups to achieve collective monitoring or management tasks. For sensitive and mission-critical sensing tasks, securing multicast applications is therefore highly desirable. To secure group communications, severalgroup key management protocols have been introduced. However, the majority of the proposed solutions are not adapted to the IoT and its strong processing, storage, and energy constraints. In this context, a novel decentralized and batch-based group key management protocol to secure multicast communications is being introduced. The protocol is simple and it reduces the rekeying overhead triggered by membership changes in dynamic and mobile groups and guarantees both backward and forward secrecy. To assess protocol,a detailed analysis with respect to its communication and storage costs are being conducted.

(Musfiq Rahman.et.al, 2010) suggests a protocol for WSN's.The design of efficient key management protocols for wireless sensor networks (WSNs) is a challenging task. To be robust and adaptable to many WSN applications, the key management protocol should not only be lightweight but also should support both pair-wise and group-wise communications. Many previous works have focused on developing efficient pair-wise key management protocols in WSNs. Very few works, however, have addressed pair-wiseand group-wise key management together using a common pre-distributed secret key. Moreover, key revocation, key material refresh, and new node addition issues have received little attention. In this paper, we propose a new key management protocol for WSNs that provides support for both pair-wise and group-wise key management with the same pre-distributed secret. The proposed protocol is efficient in terms of communication and storage overhead.

(Qing Chen.et.al, 2009) says that due to the dynamic topology and non-infrastructure, network participants cooperate with their neighbors to route packets. The lack of centralized services allows mobile ad hoc networks to be easily and swiftly deployed, but make it difficult to check others' identities on the other hand. Cryptographic tools have been introduced to secure group communications, such as private and public key infrastructure. The autonomous and distributed nature of mobile ad hoc network demands a decentralized authentication service, where public key infrastructure is considered a better solution. Public keyinfrastructure can ensure both confidentiality and authenticity, but it is impractical to provide an online trusted third party as certificate authority (CA) for mobile ad hoc network. In this paper, we proposed a new key management protocol which utilizes certificate graphs and distributed certificate authorities. Certificate graph maintained by each user represents the trust among his neighbors, then the maximum clique of certificate graph is selected to be CAs. Based on the assumption that initial certificate graph building is secure, good users have more friends while bad ones have less, thus a reliable group can be constructed. The most trustful subset of these good users -the maximum clique - is elected as the governor of this group, which takes the responsibility of certificate authentication

(D.S.Dawoud.et.al, 2009) addresses one the security problems of mobile ad-hoc network: the P2P dynamic securegroup key establishment. In the paper, a new efficient P2P hierarchal group keymanagement protocol for ad-hoc networks is being proposed. The paper introduces a two level hierarchical structure and a new scheme of group key update.

(Pawani Porambage.et.al, 2015) says that Wireless sensor networks (WSNs) are a prominent fundamental technology of the Internet of Things (IoTs). Rather than device-to-device communications, group communications in the form of broadcasting and multicasting incur efficient message deliveries among resource-constrained sensor nodes in the IoT-enabled WSNs. Secure and efficient key management is in many cases used to protect the authenticity, integrity, and confidentiality of multicast messages. This paper develops twogroup key establishment protocols for secure multicast communications among the resource-constrained devices in IoT. Major deployment conditions and requirements of each protocol are described in terms of the specific IoT application scenarios. Furthermore, the applicability of the twoprotocols is analyzed and justified by a comprehensive analysis of the performance, scalability, and security of the protocols proposed.

(Trust.T.Mapoka.et.al, 2015) suggests a distributed handover optimized authenticationscheme based on in-dependent session key per accessnetwork (HOISKA) is developed for the decentralized multiservicegroup key management scheme over wireless mobilemulticast. It enables a handover user M_i involved in multiplemulticast service subscriptions to securely reuse the longterm credential initially issued by the trusted authenticationserver (As) for deriving unique session keys per accessnetwork as it performs handover authentication acrossvarious access networks.

(T. Hardjono.et.al, 2000) suggests Intra domain group key management protocol described to support multicast groups. The domain is divided into a number of administratively scoped areas. A host-member of a multicast group is defined to reside within one (and only one) of these areas. The purpose of placing host members in areas is to achieve flexible and efficient key management, particularly in the face of the problem of changes (joining, leaving,) in the membership of a multicast group.

(B. DeCleene.et.al, 2001) says that secure group communication allows a set of nodes (or devices) to communicate securely amongst each other over unprotected and open networks. Provision of security for group communication is based on cryptographic services, which relies on careful management of cryptographic keying material. Securing group communication in wired networks is fairly well understood, however wireless networksintroduce further challenges as group members may move from one place to another while still remaining in a group session.A host mobility protocol is proposed to govern group member movement in wireless mobile environments.

(Trust T. Mapoka.et.al, 2014) tells that GKM with diverse group services subscribed dynamically by moving subscribers in wireless networks has been omitted in conventional approaches. However it is expected that significant key management overhead will arise in them due to multi services co-existing in the same network. In the paper, a scalable decentralized multi service GKM scheme considering host mobility in wireless environment is being proposed. In the scheme, authentication of mobile subscribers and key management phases are delegated from the trusted domain key distributor (DKD) to the subgroup controllers known as area key distributors (AKD).

(Kevin C. Almeroth.et.al, 1999)Multicast Backbone(MBone) is a network overlaying the internet to support multicast applications.One important characteristic of MBone is its reliance on IP Multicast which allows receivers to leave and join groups asynchronously. The MListen data collection tool was created to provide a mechanism for capturing information about when members leave and join multicast group.Of particular interestand the focus of the paper is the real use of multicastcommunication(MBone Infrastructure) to broadcast eventson a very large scale. Insight is gained by characterizingand observing the behaviour of MBone session member's .Collecting and analysing the join/leave behaviour is ofgreat benefit of understanding how any future networkinginfrastructure with multicast and real time capabilities willbe used.

(S. Mittra, 1997) examines the differences between unicast and multicast security and Iolus: a novel framework for scalable secure multicasting has been proposed. Protocols based on Iolus can be used to achieve a variety of security objectives and may be used either to directly secure multicast communications or to provide a separate group key management service to other security-aware applications. Iolus discards the idea of large at secure multicast group and replaces it with the notion of a secure distribution tree that is composed of multiple smaller secure multicast subgroups arranged in a hierarchy. Together these subgroups form a single virtual secure multicast group. The glue that holdsthe subgroups together consists of the group security agents that manage each subgroup.

(Trust Tshepo Mapoka.et.al, 2013), optimum group key management protocol for mobile multicast systems isbeing discussed. Key management is widely being adopted in securing group communicationfor both wired and wireless

networks. Securing group communication overwired networks is fairly well established; however, wireless networks bring additionalchallenges due to member mobility and increase in the number of members. The paperpresents a comprehensive survey of group key management protocols in wirelessmobile environments that employ multicast communication. They are classified intonetwork dependent and independent protocols and further categorized into tree-based and cluster-based key management protocols.

(Chung Kei Wong.et.al, 2000),a novel solution to the scalability problem of group/multicast key managementis being discussed. The paper formalize the notion of a secure group as a triple(U,K,R) where U denotes a set of users,K a set of keys held by the users, and R a userkeyrelation.Key graphs to specify secure groups are introduced. For a special class ofkey graphs,three strategies,user-oriented, key-oriented and group-oriented for securelydistributing rekey messages after a join/leave and specify protocols for joining and leavinga secure group are specified.

(D. Wallner.et.al, 1999) presents two group key management schemes,which consider mobilemembers in Mobile Network as a whole.Doing so can reduce the rekeying cost by asignificant amount when the Mobile Network moves in or out of the area comparedto existing algorithms. Proper placement of mobile members in the key tree is alsoconsidered.

(Wee Hock Desmond.et.al, 2005)proposes a protocol for facilitating member moves with consideration forbackward secrecy [15]. Using the protocol, a group member Mi moves from an areamanaged by an area key manager AKM_i (where it is currently residing), to another areamanaged by AKM_v, while still remaining in the group session. The move is managedby the DKM via AKM_i. For provision of backward secrecy, when a member movesto a visited area, the area key of visited area needs to be rekeyed. This results in groupmembers (including the moving member) residing in that particular area obtaining anew area key.

Proposed System:-

A novel GKM protocol for multiple multicast groups, called encoding based multiple group key management scheme. SMGKM supports the movement of single and multiple members across a homogeneous or heterogeneous wireless network while participating in multiple groupservices with minimized communication overheads.

A. System Design:-

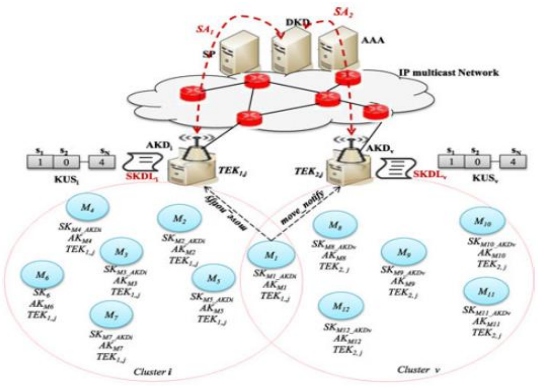

Figure ii Architecture.[1]

The framework adopts a two tier decentralized framework similar to as shown in Fig 2[1] The first level is the domain level which is the core wired part consisting of Domain Key Distributor for initial key management and authentication procedures. The second level is the area level which is the wireless part consisting of multiple clusters each of which are managed by the Area key Distributor independently. Each cluster contains a set of members subscribed to diverse multicast services who dynamicallyperform handoff across widely distributed clusters under homogeneous or heterogeneous vendors. However, the framework adopts independent TEK per cluster to alleviate 1-affect-n phenomenon and to localize rekeying process. If rekeying process of the TEK is triggered due to joins or leaves emanating from mobility, this is handled locally without disturbing the entire system. In order to unburdenthe

key management and authentication phases of the SMGKM from centralized DKD, it allow the AKDs to verify moving subscribers, generate, update and distribute the keys.Each AKD maintains secure mobility list called Session Key Distribution list to track mobility and reduce the need for rekeying when membershandoff while maintaining the subscribed services.

B. Encoding Based Key Management:-

In this key management scheme ,the keys distributed by the area key distributor to mobile nodes which has recently joined its cluster is performed by encoding operation The encoding is done with the help of 256 bit SHA-2 algorithm.SHA-2 is family of cryptographic hash functions with different block sizes, known as SHA-256 and SHA-512. They differ in word size; SHA-256 uses 32 bit words where SHA-512 uses 64 bit words. There are also truncated versions of each standard, known as SHA- 224, SHA-384,SHA- 512/224 and SHA-512/256.Like all hash functions, it takes a collection of text, computer code, or othermessage input and generates a long string oflettersand numbers that serve as a cryptographic fingerprint for that message. SHA, by contrast, is more resistant than MD5 to collisions.

C. **Rekeying Strategy:-**

To simplify the access privilege for each service, Key Update slot for N multicast services is initially by the trusted DKD on group setup depending on the number of members under G_K. The KUS format is partitioned in to slots of length l bits equivalent to N various services. Each slot l determines the total number of members from a combination of MGk participating in service N where $A_{i,N=1}$. Moreover,each slot can dynamically increment or decrement by 1 whenever a join or leave occur respectively or reset to zero if no member is subscribed to service N.

D. Transmission:-

Assuming the SP hold valid $TEK_{i,j}$ shares, it securely transmit the services subscribed to the corresponding M_i under each cluster using a specific bandwidth for that service. Let $BW(S_N)$ denote the bandwidth used to transmit service S_N, let $C(N_{G_k})$ be the cost of transmitting a unit data to n members M_i for i = 1 ...n in G_k via multicast. Two methods that can be used to efficiently transmit the servicesillustrated in Fig i to the corresponding M_i inG_k. In method 1, the total communication cost (TCMETHOD1) of transmitting the multicast services can be evaluatedas:

$$TCMETHOD1 = BW(S_N).C\sum_{i=1}^{k} N_{G_k} \qquad (1)$$

In method 2, the total communication cost (TCMETHOD2) of transmitting the multicast services can be evaluated for each service as

$$TCMETHOD2 = C\left(N_{G_k}\right).C\sum_{I=1}^{N-1} BW(S_N) \qquad (2)$$

Therefore SMGKM can transmit multiple services with optimised bandwidth utilization without sacrificing security using TCMETHOD2 with aggregated service band width. However the conventional approaches use TCMETHOD1 which require huge bandwidth for secure data transmission. However TCMETHOD1 can be optimized by applying tree based approach.

Result and Discussion:-

The performance evaluation is done in a simulated environment using NS2.Three heterogeneous networks- UMTS, Wi-Fi, WiMAX are created. Each network has some number of nodes. Some nodes have been kept as static while other nodes are kept as mobile. When a node moves from one network to another the keys are changed as per the rekeying and the rekeying is localized. Simulation isdone by using the network simulator NS2.NS2 stands for Network Simulator Version 2.It is an open source event driven simulator designed especially for research in computer communication networks. The analysis is done mainly on the basis of the three factors namely Communication overhead, Packet Delivery Ratio, and Throughput.

A. Communication Overhead:-

Communication overhead can be defined as the overhead incurred while communicating the keys between the AKD and particular nodes. This overhead corresponds to the expected amount of rekeying messages from unicast or multicast transmissions at the cluster level when N subscribers perform handoff while maintaining S-active multicast sessions.

.

$$Communication\ Overhead = O(n) + s \qquad (3)$$

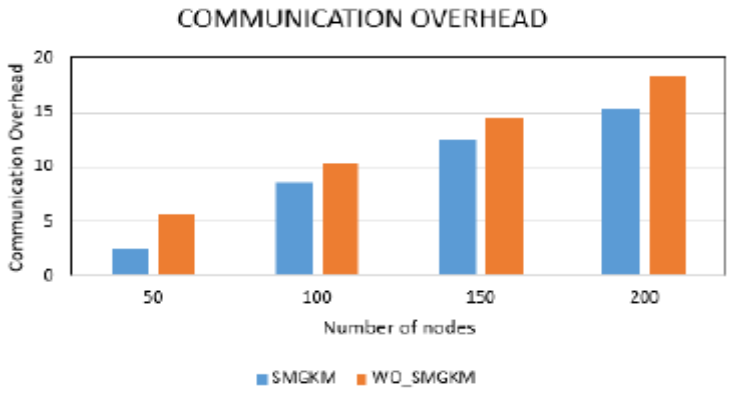

Figure iii Communication Overhead.

Communication overhead involves the overhead incurred in communication between the DKD and AKD.Since the communication is always between the AKD and the nodes in a particular clusters therefore the communication overhead incurred is less in SMGKM scheme than in otherconventional schemes without SMGKM is shown in fig iii.

B. Packet Delivery Ratio:-

Packet Delivery Ratio is the number of packets deliveredto the destination.It can be defined as the ratio of numberof received packets to the number of send packets.Since inSMGKM scheme,the fig iv shows that the packet deliveryratio is high than in other schemes.

$$PDR = \frac{no.\ of\ pkt\ received}{no.\ of\ pkt\ sent} * 100 \qquad (4)$$

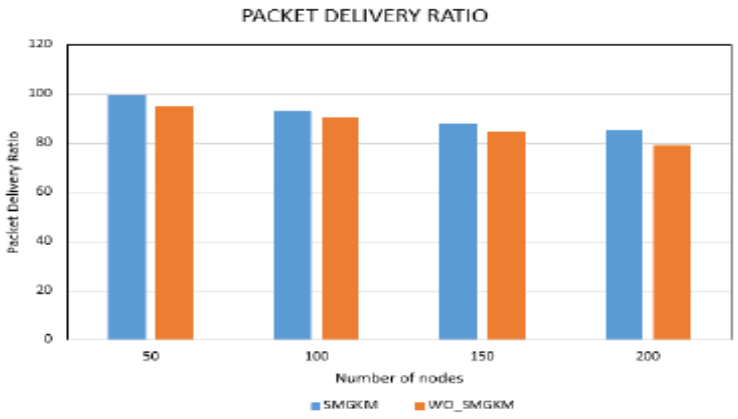

Figure iv Packet Delivery Ratio

C. Throughput:-

Throughput is the rate at which something can be processed. It can be defined as the rate of successful message delivery over a communication channel. Throughput is usually measured in terms of bits per second (bit/s or bps) and sometimes in data packets per second (p/s or pps) or data packets per time slot. Throughput is high in SMGKM other than conventional schemes as shown in fig v.

$$Throughput = \frac{No.of\ byte\ received * 8}{endtime - starttime} \quad (5)$$

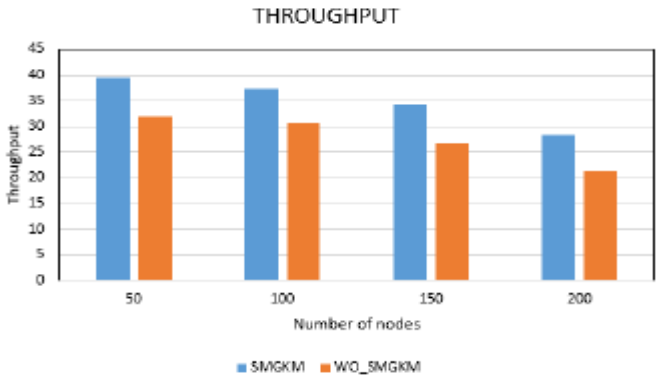

Figure v Throughput

Conclusion:-

Key establishment is a key issue in secure communication. Here an encoded 256 bit hash based Slot multiple key management scheme is being established.The scheme has been proposed to improve the key management performance in the presence of multi- moves participating in multi groupservices. It considered providing backward confidentialitywhere mobile receivers dynamically perform handoffwhile seamlessly maintaining diverse subscriptions.In contrast to convectional schemes targeted for a singleservice, SMGKM used a new rekeying strategy based onlightweight KUS and SKDL for effectively performing key management and authentication phases respectively duringhandoff. SMGKM adopted independent TEK per cluster tolocalize rekeying and mitigate one-affect-n phenomenon. Byoffloading the key management and authentication phasesto the intermediate AKDs massively reduced signalling loadat the core network than in convectional schemes hencegiving DKD scalability while preventing bottlenecks.Resultsof the SMGKM performed much better in comparison toprevious works.

References :-

1. **Trust T. Mapoka, Simon J. Shepherd and Raed A. Abd-Alhameed**, A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast, IEEE Transactions on Mobile Computing, Vol. 14,No. 8, August 2015.
2. **Mohammed Riyadh Abdmeizeim, Djamel Tandjaoui and Imed Romdhani,** A decentralized Batch- Based Group Key Management Protocol for Mobile Internet of Things, IEEE International Conference onComputer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015.
3. **Musfiq Rahman, Srinivas Sampalli and Sajid Hussain,** A robust pair-wise and group key management protocol for wireless sensor network, IEEE Globecom Workshops, pp: 1528-1532,2010.
4. **Qing Chen, Xiadong Lin, Sherman Shen and Kazuo Hashimoto,** A Group-Based Key Management Protocol for Mobile Ad Hoc Networks, IEEE Global Telecommunications Conference, pp: 1-5, 2009.
5. **D.S.Dawoud, S.H.Mneney, Farhad Aghdasi and Peter Dawoud,** An efficient hierarchical group key management protocol for mobile ad-hoc networks,1st International Conference onWireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology, 2009.
6. **Pawani Porambage, An Braeken, Corinna Schmitt, Andrei Gurtov, Mika Ylianttila, and Burkhard Stiller, Group** Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications, IEEE Access, vol 3, pp: 1503-1511, 2015.

7. **S.Rafaeli and D.Hutchison**,A Survey of Key Management for Secure Group Communication, ACM Computing Surveys, Vol. 35, No. 3, September 2003.
8. **Trust T. Mapoka, Simon J. Shepherd and Raed A. Abd- Alhameed**, Handover Optimised Authentication Scheme forHigh Mobility Wireless Multicast, 17th UKSIM- AMSS International Conference on Modelling and Simulation,2015.
9. **T. Hardjono, B. Cain, and I. Monga**, Intra-domain group key management for multicast security, IETF Internet draft, Sept. 2000.
10. **DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, S. Vasudevan, and C. Zhang**,Secure group communications for wireless networks in Proc. Commun. Netw. - Centric Oper. Creating Inf. Force. IEEE Military Commun. Conf., 2001, vol. 1, pp. 113-117.
11. **Trust T. Mapoka, Yousef. A.S. Dama, Haider M. AlSabbagh, Simon J. Shepherd and Raed A. Abd-Alhameed**,Multi-Service Group Key Establishment for Secure Wireless Mobile Multicast Networks, Journal of Telecommunications, Volume 27, Issue 2, October 2014.
12. **Kevin C.Almeroth,Mostafa H.Ammar**,Multicast group behaviour in the Internet's multicast backbone (MBone),Networking and Telecommunications Group,November 5 1999.
13. **S. Mittra**,Iolus: A framework for scalable secure multicasting,Proceedings of the ACM SIGCOMM, vol. 27, no. 4, pp. 277-288, New York, Sep. 1997.
14. **Trust Tshepo Mapoka**,Group Key Management Protocols for Secure Mobile Multicast Communication: A Comprehensive Survey, International Journal of Computer Applications, vol.84,no.12,December 2013.
15. **Chung Kei Wong,Mohamed Gouda, and Simon S. Lam**,Secure Group Communications Using Key Graphs,
16. IEEE/ACM Transactions on Networking, Vol. 8, No. 1,February 2000.
17. **G. S. V. R. K. Rao and G. Radhamani**,WiMax: A Wireless Technology Revolution, USA:Auerbach Publishers, 2008.
18. **3GPP**,Multimedia Broadcast/Multicast Service; Stage 1 (Release 8), Technical Specification 3GPP TS 22.146, vol. 8.3.0, (2007-06),Jun. 2007.
19. **Wallner, E. Harder, and R. Agee**,Key Management for Multicast: Issues and Architecture, National Security Agency,RFC 2627, Jun. 1999.
20. **Wee Hock Desmond Ng, Zhili Sun, Haitham Cruickshank**, Group Key Management with Network Mobility, IEEECommunication Magazine,2005.