International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
Volume 2 Issue 1 –OCTOBER 2013.

Efficient Position-Based Opportunistic Routing Using Reliable Data Delivery in MANET

M. Geetha[#1], D. Renuka[*2]

[#]*Associate Professor, Dept. Of Computer Application, Muthayammal College of Arts & Science*
[2] renulatha214@gmail.com
[*] *Dept. Of Computer Application, Muthayammal College of Arts & Science*

***Abstract*- While satisfying security requirements is crucial for secure group communications in wireless systems; mobile group applications often have application-specific performance requirements in terms of timeliness, reliability, and system reconfigurability. Often there exists a tradeoff between security versus performance goals since security protocols may introduce undue computational and network overheads which may prevent performance goals from being met. Many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. The cluster head election is invoked on-demand, and is aimed to reduce the computation and communication costs. A large variety of approaches for ad hoc clustering have been developed by researchers which focus on different performance metrics. This paper presents a survey of different clustering schemes.**

Index Terms*- *MANETS, location privacy, Clustering, Group Key, Key Management Protocol.

I. INTRODUCTION

An ad hoc network is an assortment of independent nodes that communicate with each other, most regularly using a multi-hop wireless network. Nodes do not inevitably know each other and come together to form an ad hoc group for some particular reason. Key distribution systems typically involve a trusted third party (TTP) that acts as an intermediary between nodes of the network. A node in an ad hoc network has straight connection with a set of nodes, called neighboring nodes, which are in its communication range. The number of nodes in the network is not essentially preset. New nodes may join the network while existing ones may be compromised or become un-functional [1]. Key management in the ad hoc network is a challenging issue concerning the security of the group communication. Group key management protocols can be approximately classified into three categories; centralized, decentralized, and distributed [2].

MANET is one where there is no predetermined infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other‘s radio range communicate directly by means of a wireless network, whereas those far apart rely on other nodes to act as routers to relay its messages [3]. The most suitable solution to provide the services among which authentication, data integrity and data confidentiality is the establishment of a key management protocol. This protocol is liable for the generation and the distribution of the traffic encryption key (TEK) to all the members of a group. This key is used by the source to encrypt multicast data and by the receivers to decrypt it. Therefore only legitimate members are able to receive the multicast flow sent by the group source [4]. The elemental security services provided by every key management system are key synchronism, secrecy, freshness, independence, authentication, confirmation and forward and backward secrecy [7].

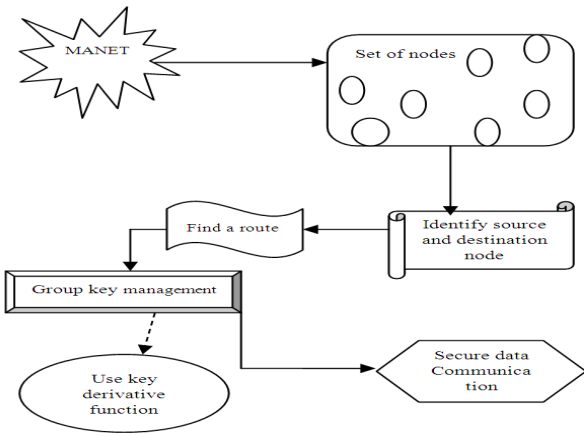
Cluster-based routing is a solution to address nodes heterogeneity, and to limit the amount of routing information that propagates inside the network. The idea behind clustering is to group the network nodes into a number of overlapping clusters. Clustering makes possible a hierarchical routing in which paths are recorded between clusters instead of between nodes. This increases the routes lifetime, thus decreasing the amount of routing control overhead. Inside the cluster one node that coordinates the cluster activities is cluster head (CH). Inside the cluster, there are ordinary nodes also that have direct access only to this one cluster head, and gateways. Gateways are nodes that can hear two or more cluster heads.

The group key may be distributed by a key server that provides group key management services. A dedicated key server may be employed, or the functionality may be implemented on a server offering other services such as authentication. Multiple key servers may co-exist in a clustered network, where a cluster head may play the role of a key server. The group key is employed to encrypt messages sent by a member to the group. Only members of the group with the group key are capable of decrypting the messages. Key generation along with key distribution has been a central issue in key management for secure group communications. Over the years many key management protocols have been proposed and studied (see Chapter 2 Related Work). In particular, in MANETs with no infrastructure support, since a key server does not exist, key management must be performed in a fully distributed manner. This adds to the system overhead whenever the group key is “rekeyed” due to group member leave/join/eviction events. To deal with insiders

attacks, intrusion detection system (IDS) techniques may be used to detect compromised nodes and to evict such compromised nodes to prolong the lifetime of the GCS. 2

While satisfying security requirements is crucial for secure GCSs in wireless systems, mobile group communicating applications often have application-specific performance requirements in terms of timeliness, throughput, delay, and traffic capacity. These application requirements are generally referred to as the quality of service (QoS) requirements, including both security and performance requirements in the context of mobile GCSs. By "QoS-aware" protocols, we refer to those protocols being designed to satisfy both security and performance requirements of the system. These QoS-aware protocols are adaptive in nature with designs incorporated to allow the system to adapt to dynamic situations by adjusting operational settings under which both the system's security and performance requirements can be best satisfied.

II. PROPOSED WORK



Region-based group key management protocol divides a group into region-based subgroups based on decentralized key management principles. This partitioning of region into subgroups improves scalability and efficiency of the key management scheme in providing a secure group

communication. Figure 1 shows the partitioning of region into subgroups on the basis of decentralized key management principles [16]. It is assumed that each member of the group is

equipped with Global Positioning System (GPS) and therefore each one knows its location as it moves across the regions. For secure group communications, all members of a group share a secret group key, KG. In addition to ensure security in communication between the members of each subgroup all the members of the subgroups in the region hold a secret key KR_i. This shared secret key is generated and managed by a distributed group key management protocol that enhances robustness. This region-based group key management protocol will function at the optimal regional size recognized to reduce the cost of key management in terms of network traffic. The nodes should have the following keys: MK, which is shared by all the nodes in the network; LK, which is shared with the BS; and SK, which is shared with another node. Each of these keys is considered in turn with the reasons for including it in the prototype.

Master key (MK): This is a globally shared key that is used by the base station for encrypting messages that are broadcast to the whole group. Each node is imprinted with master key and LAFs when it is manufactured.

Local key (LK): Every node has a unique key that is injected with initial local key (LK), is shared with the base station. This key is the basic parameter for the re-keying function of the

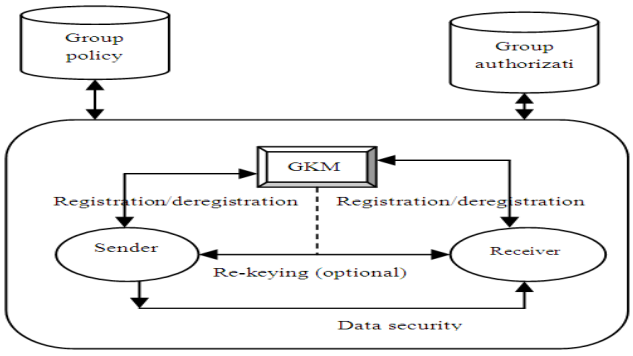
proposal and is used for secure communication between the node and the base station.

Session key (SK): Every node shares an SK with each of its immediate neighbours. In NRFP, SKs are used for securing communications that require privacy or source authentication.

LAFs: The local administrative functions include master function', re-keying function', and derivation function' and can be imprinted with node to achieve a high-level security of node -

to- node communication. The LAFs are responsible for key generation of the cluster session keys depending on which initial master key and local control key were imprinted at the time of manufacturing, whereas the HMAC is adopt of LAFs work. Master function, the derivation function is used to generate new key values based on requesting message coming from BS or CH. The re-keying process is necessary for two reasons:

Group Key management data security model



The main characteristics of GKM for data security are as follows:

1. It efficiently presents privacy and substantiation, replay protection and DoS protection from attacks.
2. An efficient rekeying once transforms in group membership.
3. A consistent deliverance of rekey messages.
4. A high throughput and low latency.

Messages required for IDS activities follow the rules for group communication, including status exchange, vote-participant selection, vote-participant-list dissemination and vote dissemination. A target node is examined by IDS periodically and if the target node is considered compromised, it will be evicted by rekeying the group key ***KG*** based on GDH.

For typical group communication, we accept to use the publish/subscribe service. It is assumed that all members are interested in all published data by all members. Thus, all published data in each member are disseminated to all members whenever each node publishes its data. By taking two-level hierarchical key management structure, the published data in each node is broadcast to its members in the region, and then the leader receiving the published data distributes it to other leaders. After then, each leader broadcasts the published data to its members respectively. When all published data are disseminated to all members in this way, a group key is used to encrypt/decrypt the published data.

III. CONCLUSION

In the case of communication hole, we propose a Virtual Destination-based Void Handling (VDVH) scheme in which the advantages of greedy forwarding (e.g., large progress per hop) and opportunistic routing can still be achieved while handling communication voids. To work with the multicast forwarding style, a virtual destination-based void handling scheme is proposed. By temporarily adjusting the direction of data flow, the advantage of greedy forwarding as well as the robustness brought about by opportunistic routing can still be achieved when handling communication voids.

IV. REFERENCES

[1] [1] A. Renuka, and K. C. Shet, “Cluster Based Group Key Management in Mobile Ad hoc Networks,” IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 4, pp. 42-49, 2009.

[2] [2] S. Rafaeli, and D. Hutchison, “A survey of key management for secure group communication,” ACM Computing Surveys, vol. 35, no. 3, pp. 309–329, 2003.

[3] [3] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, “Security in mobile Ad-Hoc networks-Challenges and Solutions,” IEEE Transactions on Wireless Communications, vol. 11, no. 1, pp. 38-47, 2004.

[4] [4] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor, “Group Key Management in MANETs,” International Journal of Network Security, vol. 6, no. 1, pp. 67-79, 2008.

[5] [5] L. Lazos, and R. Poovendram, “Energy-aware secure multicast communication in Ad Hoc networks using geographical location information,” in IEEE International Conference on Acoustics Speech and Signal Processing, pp. 201-204, 2003.

[6] [6] J. E. Wieselthier, G. D. Nguyen, and A. Ephremides, “On the construction of energy-efficient broadcast and multicast trees in wireless networks,” in INFOCOM 2000, pp. 585-594, 2000.

[7] [7] Menezes, P. V. Oorschot, and S. A. Vanstone, “handbook of Applied Cryptography”, CRC Press, New York, 1997.

[8] [8] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, “A Cluster-Based Security Architecture for Ad Hoc Networks,” *Proceedings of 23rd IEEE INFOCOM*, vol. 4, March 2004, pp. 2393-2403.

[9] [9] C. Becker and U. Wille, “Communication Complexity of Group Key Distribution,” *Proceedings of 5th ACM Conference on Computer and Communications Security*, San Francisco, CA, 2-5 Nov. 1998, pp. 1-6.

[10] [10] G. Bianchi, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function,” *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, March 2000, pp. 535-547.