International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 5, May-2014, pp: (176-180), Impact Factor: 1.252, Available online at: www.erpublications.com.

An Efficient Secure group key management system in wireless ad hoc network

S. Arun kumar[1], K. Balasubramanian M. E.[2],
[1]P.G. Student Department of C.S.E, E.G.S. Pillay Engineering College, Nagapattinam, Tamilnadu, India
[2]Assistant Professor, Department of C.S.E, E.G.S. Pillay Engineering College, Nagapattinam, Tamilnadu, India

Abstract: The problem of efficiently and securely broadcasting to remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation center, and the dynamics of the sender. The existing key management paradigms cannot deal with these challenges effectively. This paper proposes and specifies a protocol for distributing and managing secure group keys in ad hoc environments, which applies for the Secure Optimized Link State Routing Protocol (SOLSR). Our protocol manages group keys taking into consideration the frequent network partitions and the absence of infrastructure. The analysis shows that the protocol is energy efficient for high key replacement rates and frequent network partitions. We have using an Energy Efficient Group key management (EEGK) for secure data processing on network. A provably secure protocol in the new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks. In the proposed protocol after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexity, even in the case of member changes or system updates for rekeying.

Index Terms: SOLSR, EEGK, MANET, IDs.

Introduction

Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a pre existing communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. Key management is a challenge in ad hoc networks because it is not possible to guarantee the availability of a resource to all nodes at any time. Hence, ad hoc networks cannot base its authentication system in centralized and fixed infrastructure. Furthermore, ad hoc networks usually are composed by nodes with constrained devices. Hence, security must be provided without large energy consumption, because some nodes cannot execute frequent complex cryptographic operations. The key management is the process of maintaining the secret key between the sender and receiver. Using this key the sender can encrypt the data which is transmitted to the receiver and send it with the security key to decrypt the message. The receiver decrypts the transmitted message from sender using that security key. This method of communication will give confidentiality and integrity in the data transmission.

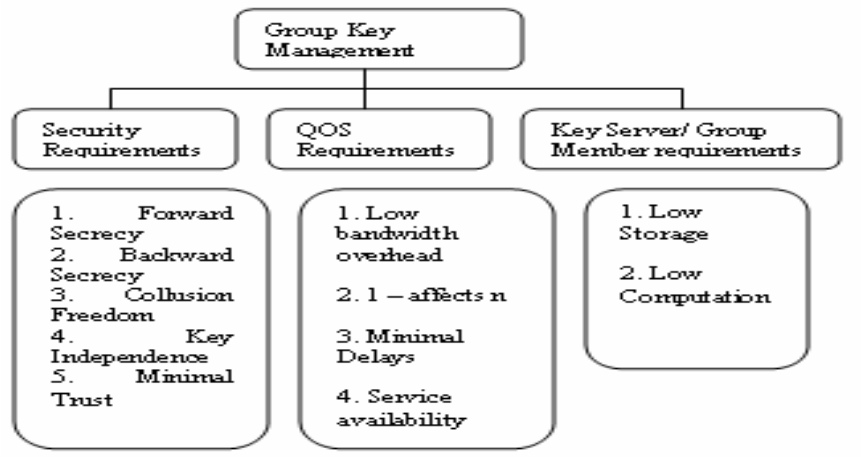

Fig 1: Group Key management Techniques

Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal operation. Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

II. RELATED WORK

There are many approaches has been discussed in the past for key management of categorical data's, we explore few of them in this chapter to find the prose and corners of the methods proposed. In wireless Mesh Network the security is provided by using the An Attack Resilient Security Architecture. ARSA eliminates the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. ARSA supports efficient mutual authentication and key agreement both between a user and a serving WMN domain and between users served by the same WMN domain [1]. ARSA is more practical and lightweight because it does not require a WMN operator to establish pair wise bilateral SLAs and interact in real-time with potentially numerous other WMN operators. ARSA is also a homeless solution in which each user, instead of being bound to any specific WMN operator, can get ubiquitous network access by a universal pass issued by a third-party broker.

PEACE, a novel Privacy-Enhanced yet Accountable security framework, tailored for WMNs. It enforces strict user access control to cope with both free riders and malicious users. It also offers sophisticated user privacy protection against both adversaries and various other network entities. PEACE is presented as a suite of authentication and key agreement protocols built upon our proposed short group signature variation [2]. PEACE enforces strict user access control to cope with both free riders and malicious users using the following key agreement protocol 1.user-router mutual authentication and key agreement protocol 2.User-User Mutual Authentication and key Agreement

A pyramidal security model contains a set of hierarchical security groups and multicast groups. Three schemes have been implemented in MANET to provide pyramidal security model [3], [2]. The schemes are: separated star key graph, separated tree key graph, and integrated tree key graph. The first two key graphs are derived from legacy single-security-level multicast key management schemes without considering the relationship among different multicast groups. The integrated tree key graph is designed to utilize only one tree key graph to manage all the multicast groups and thus achieve satisfying overall performance. The integrated tree key graph is a sorted recursive tree; it cannot adopt the existing tree balancing approaches for an individual tree key graph.

A cooperative caching scheme specifies how multiple nodes share and manage cached data in a collaborative manner. For multimedia caching in mobile computing environments, Data copy is primary if it is not available within the neighborhood. Otherwise, the data copy is secondary. The range of neighborhood is provided as a customizable option. The reason of discriminating primary and secondary data is that cache miss cost is proportional to the travel distance of a data request, and primary data usually incur higher cache miss cost than secondary data [4].

III. PROPOSED WORK

The group key distribution mechanism replaces the group key periodically or when a node is excluded. The periodic distribution excludes adversaries which possess the group key, but not a private key. For instance, in community networks, an authorized user may send the group key to a non-authorized friend in order to the friend accesses network resources. The group key distribution is also triggered by an intrusion detection system (IDS). When the IDS send an alert, it means that there is an adversary that should be excluded.

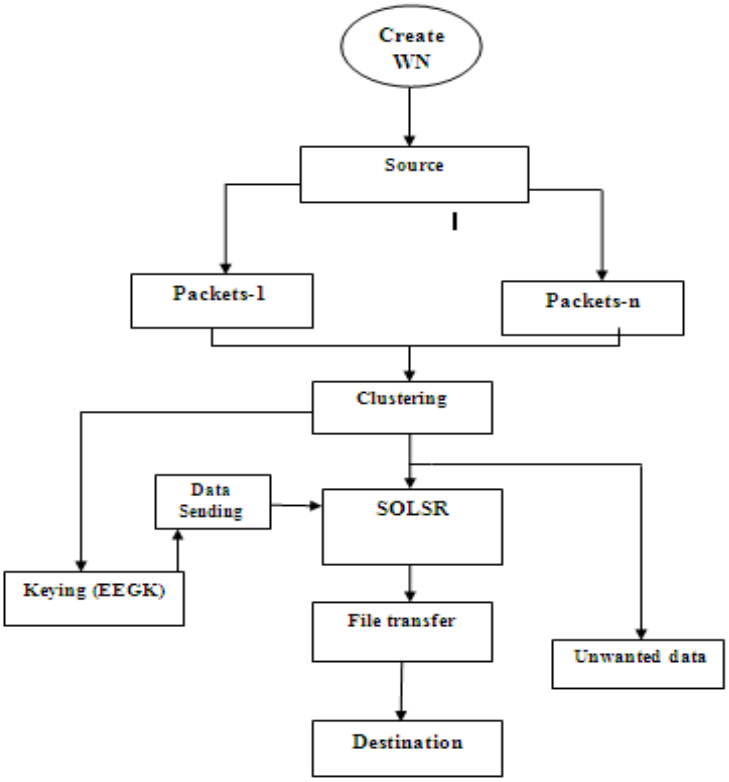

Fig 2: Architecture of Proposed system

The symmetric-key broadcast encryption, public–key broadcast encryption. In the symmetric-key encryption only the trusted center generates all the secret keys and broadcast message to the users. Hence, only the key generation center can be the broadcaster or the sender. In the public key encryption in addition to secret key for each user, the trusted center also generates a public key for all users so that any can play the role of broadcast or sender. In this communication the data transmitted in an unsecured network. The non authorized user may intercept the communication between the nodes and also possible to change the content of transmitted message. Due to these the integrity of the communication will degrade. In order to maintain good consistency communication between the sender and the receiver the key management process is introduced. The key management is the process of maintaining the secret key between the sender and receiver. Using this key the sender can encrypt the data which is transmitted to the receiver and send it with the security key to decrypt the message. The receiver decrypts the transmitted message from sender using that security key. This method of communication will give confidentiality and integrity in the data transmission.

3.1 Clustering on network:

Clustering is an important mechanism in large multi-hop wireless sensor networks for obtaining scalability, reducing energy consumption and achieving better network performance. Most of the research in this area has focused on energy-efficient solutions, but has not thoroughly analyzed the network performance, e.g. in terms of data collection rate and time. The main objective of this paper is to provide a useful fully-distributed inference algorithm for clustering, based on belief propagation. The algorithm selects cluster heads, based on a unique set of global and local parameters, which finally achieves, under the energy constraints, improved network performance.

IV. RESULTS AND DISCUSSION

The Java Platform is the concept of a "virtual machine" that executes Java byte code programs. This byte code is the same no matter what hardware or operating system the program is running under. There is a JIT compiler within the Java Virtual Machine, or JVM. The JIT compiler translates the Java byte code into native processor instructions at run-time and caches the native code in memory during execution. The use of byte code as an intermediate language permits Java programs to run on any platform that has a virtual machine available. The use of a JIT compiler means that Java applications, after a short delay during loading and once they have "warmed up" by being all or mostly JIT-compiled, tend to run about as fast as native programs. Since JRE version 1.2, Sun's JVM implementation has included a just-in-time compiler instead of an interpreter although Java programs are Platform Independent, the code of the Java Virtual Machine (JVM) that execute these programs are not. Every Operating System has its own JVM.

We analyzed the energy consumption of EEGK and of group key agreement protocols, considering energy constrained devices. The energy costs with cryptographic operations are relative, designed for embedded low-power environments. We choose RSA with 1024-bit key, Advanced Encryption Standard (AES) with 128-bit key and keyed-Hash Message Authentication Code with 128-bit key as cryptography functions, because they are well-known and largely used. We estimate the average number of messages sent and received by each node and the number of cryptographic operations carried out. Our scenario, which is denser than one of a community network, is composed of nodes. We consider that the average number of neighbors of each node is approximately constant even with the mobility.

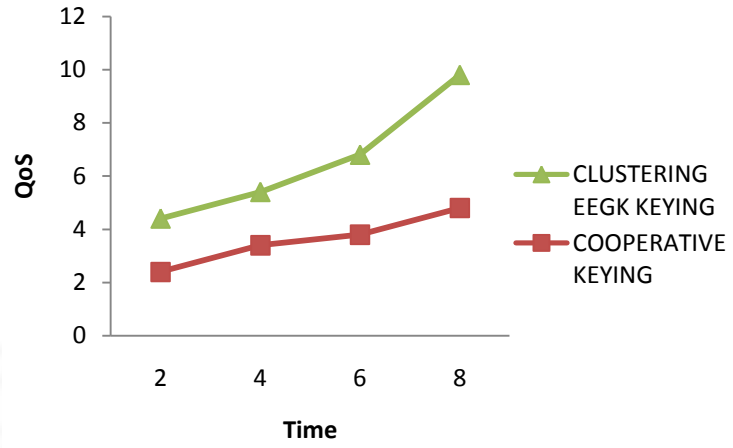

Fig: 2 Quality of service

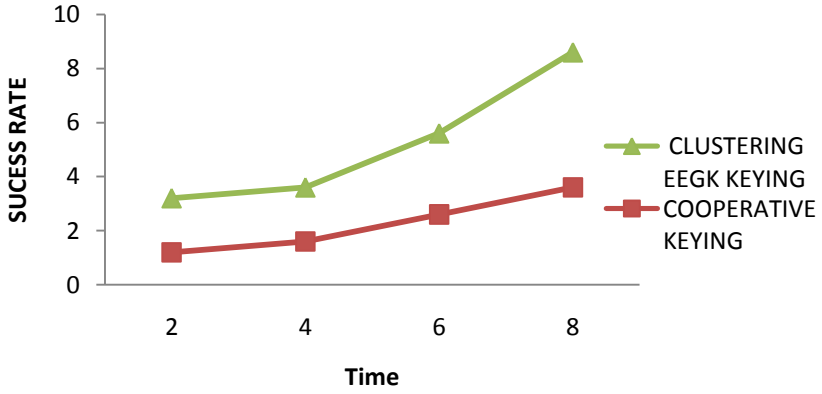

Fig: 3 Success rate on network

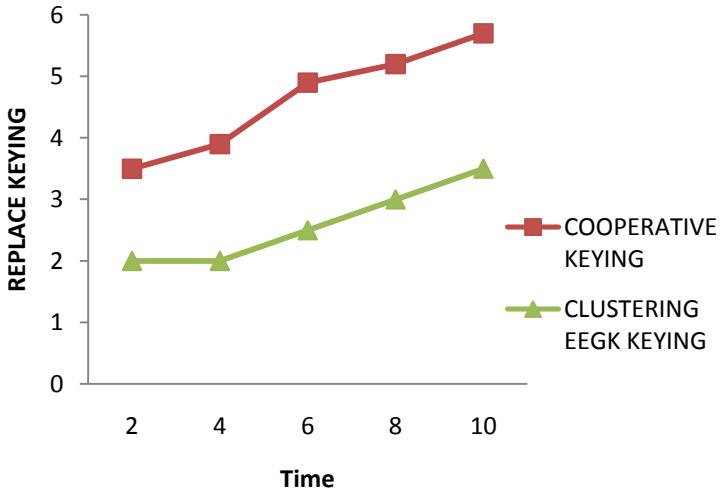

Fig: 4 Replace Keying

V. CONCLUSION

In this paper, we presented and evaluated the Energy Efficient Group key management for Secure Routing (EEGK). Our protocol restricts non-authorized access to the network through periodic and triggered group key replacement. EEGK with SOLSR makes ad hoc routing more secure against non-authorized nodes with a small energy cost, even if there is collusion between authorized and non-authorized nodes. Moreover, the proposed protocol synchronizes the new group key use and is robust against node failures and network partitions. The use of an intrusion detection system increases the security provided by EEGK, because non-authorized nodes that utilize the private key of some authorized node to obtain the new group key are also excluded from network.

VI. REFERENCES

[1]. Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916–1928.
[2]. K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203–215.
[3]. B.Rong, H.-H.Chen, Y.Qian, K.Lu, R.Q.Hu, andS.Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study," IEEE Trans. Technol., vol. 58, no. 1, pp. 398–408.
[4]. Y.-M. Huang, C.-H, T.-I. Wang and H.-C. Chao, "Constructing secure group communication over wireless ad hoc networks based on a virtual subnet model," IEEE Wireless Commun., vol. 14, no. 5, pp. 71–75.
[5]. L.Zhang, Q.Wu, A.Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Technol., vol. 59, no. 4, pp. 1606–1617.
[6]. M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," Adv. Cryptol., vol. 950, EUROCRYPT'94, LNCS, pp. 275–286,
[7]. Y.Amir, Y.Kim, C.Nita-Rotaru, J.L.Schultz, J.Stanton, andG. Tsudik, "Secure group communication using robust contributory key agreement," IEEE Trans. Parallel Distributed. Syst., vol. 15, no. 5, pp. 468–480.
[8]. Y. Sun, W. Trappe, and K. J. R. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," IEEE/ACMTrans. Network, vol. 12, no. 4, pp. 653–666.
[9]. D.Suganya Devi, "Secure Multicast Key Distribution for Mobile Adhoc Networks", Vol. 7, No. 2, 2010.
[10]. Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", 2011.
[11]. Hongmei Deng, Annindo Mukherjee, "Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks"
[12]. Joseph Binder, "Decentralized Key Management in Ad Hoc Networks"2010.
[13]. Joao P. Vilela and Joao Barros, "A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks", 2011.