EFFECTIVE KEY MANAGEMENT SCHEME IN MOBILE AD HOC NETWORK

Abstract :- In mobile ad hoc network secure communication is more challenging due to dynamic technology and mobility of nodes. In order to design practical and sufficient management scheme to understand the features of ad hoc network and why traditional key management system can not be used. The main idea of key management is to provide secure methods for handling cryptographic keying algorithm. The main purpose of key management includes key for generation, distribution and maintenance. Key maintenance include the process for key storage, update, key revocation etc. there are so many key management schemes have been proposed for MANET'S. The main purpose of this paper is to show some solution for key management in MANET'S and propose a new group key management scheme namely a hierarchical, simple, efficient and scalable group key based on clustering management scheme for MANET'S and different other scheme are classified.

Keywords- Group key management ; MANETs security; key management approach for MANET'S.

1. Introduction

Mobile ad hoc network is a kind of mobile multiple hops and self discipline system that not depend on the fixed communication facilities. MANET'S is a series of nodes connected through wireless network, Each network node has the double function as terminal and routers. The nodes are peer-to-peer communication through a high degree of coordination. MANET have the ability to form on the fly and dynamically handle the joining or leaving of nodes in the network.

MANET's have the following characteristics.

Dynamic Network Topology:- Mobile ad hoc network nodes are mobile and technology of the network may change frequently. Nodes may have around within MANET'S can also partitioned into multiplier smaller network or be merged with other network.

Limited Bandwidth :- The use of wireless communication currently used a lower bandwidth than traditional networks. This may limit the number and size of the message sent during protocol execution.

Energy Constrained Nodes:- Nodes in MANET will most often rely on batteries as their power source. Use of complex algorithms that consumes CPU time and energy there may not be possible.

Limited Physical Security:- By definition of mobile ad hoc network does not have any fixed infrastructure, All networks function are performed by the nodes themselves is a self organizing manner.

Because of this reason securing ad hoc networks is challenging. One of the major problems in providing security services in ad hoc networks is how to manage the cryptographic keys that are needs

2. Key Management

MANET security is based on the use of proper key management system. Network security depends in many cases on proper key management. Key management services must provide solutions to be able to answer the following questions: Trust model, Cryptosystems, Key creation, Key storage and Key distribution. The key management service must be ensure that the generated key are securely distributed to their owners. Key must be kept secret, so that confidentiality, authenticity and integrity are not violated. Symmetric keys are applied, both or all of the parties involved must receive the key securely. Public key cryptography the key distribution mechanism must guarantee that private keys are delivered only authorized parties. We show some solution for key management in ad hoc network.

3. Application of Mobile Ad Hoc network

Ad hoc networks have application in two major fields: Military and Commercial environment. Early 1970s with the DARPA and PRNET project, where the initial focus was on Military Application. MANET is particular attractive because of their lack of infrastructure and self configuration nature. Its application such as sensor networks, positional communication systems and tactical ad hoc networks will continue to be some of the driving forces behind ad hoc network development. The presence absence of priori security relationship has a fundamental impact on the design strategy of key management scheme for MANET.

Commercial ad-hoc network may include establishing connectivity in terrains where conventional networks, such as cellular networks, are not financially viable, cannot provides sufficient coverage, or need bypassing. Private or personal area networks are possible application of ad hoc networks. It is anticipated that these application will gain momentum as soon as the flexibility and convenience of self organized ad hoc networking fully apperecited and protocols are implemented with commercially available products. Such as cellular networks that was once seen as an impractical technology has now become a necessity. It also include Emergency situation, Natural or Man-made disaster, vehicular ad-hoc networks.

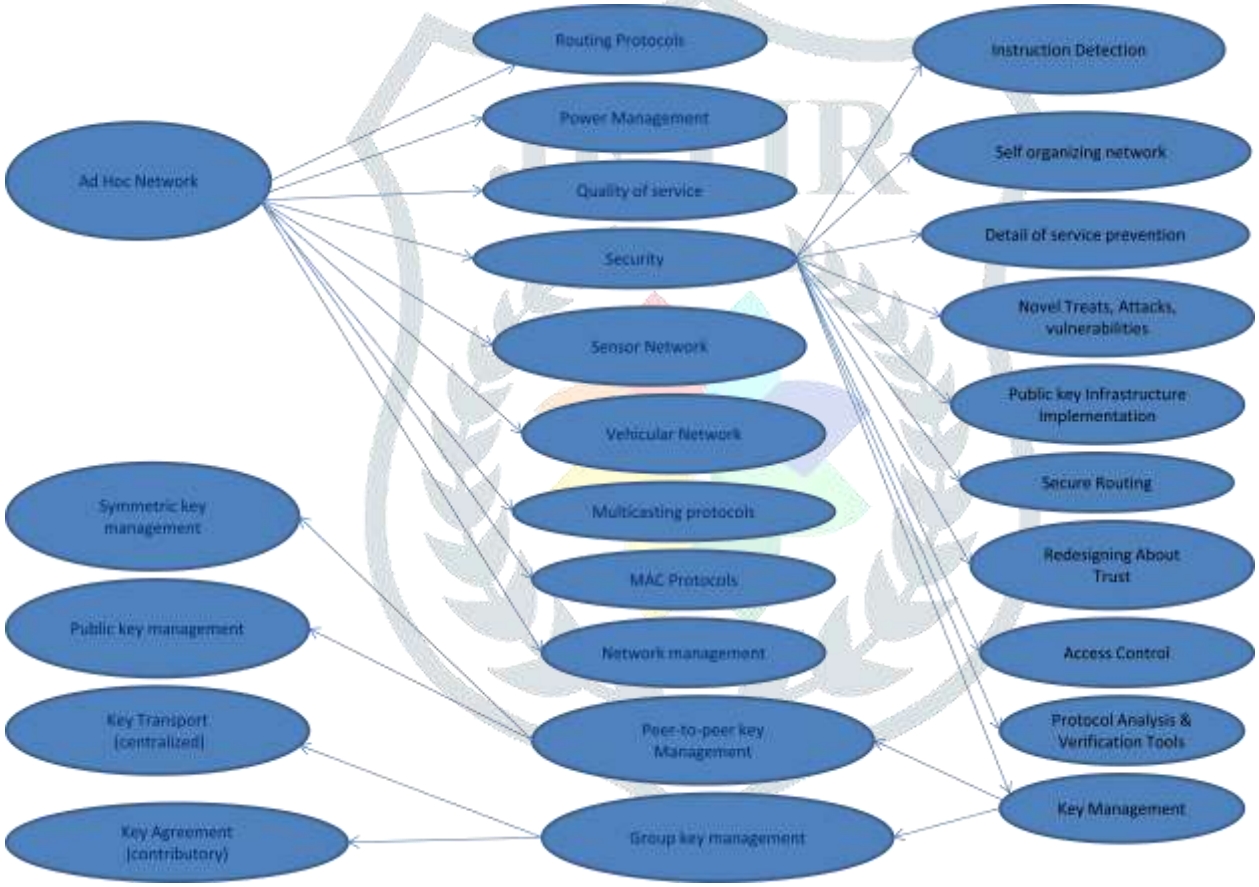
4. Key Management In MANETs

In this paper we considers the classification of security problems in MANETs. The main idea is to position the problem of peer-to-peer key management within the MANET security field. The main observation is that cryptographic techniques are often at the center of solving security problems in MANETs and hence need key management. The subsequent topics also provide definitions and terminology for the different properties and requirements of key management schemes.

4.1 . Motivation for Key Management in Mobile Ad Hoc Networks

The evolution of MANETs over the past decade, there are still a number of security-related problems that are open. It means that, although solutions have been proposed, none seems to satisfy all of the constraints of MANETs. In Figure 1 show the areas investigated within the MANET field, with particular focus on security issues. In this figure highlights the main areas of ad hoc network security and could be expanded. As per Figure 1, research in theMANET security field is concerned with a variety of different aspects. Researchers in the ad hoc network security field initially focused on secure routing protocols (like SEAD, ARAN, SRP).

- To provide a routing mechanism that is robust against the dynamic network topology of MANETs.
- To provide a routing mechanism that offers protection against malicious nodes.



Routing protocols may use many security techniques to mitigate attacks on the routing infrastructure. Some of these techniques are redundancy exploitation; diversity coding; on-demand route discovery; route maintenance techniques;fault- or intrusion-tolerant techniques, and cryptographic techniques

For example, routing schemes may exploit redundancy by establishing multiple routes from source to destination (as easily achieved by ZRP, DSR , TORA, and AODV) By sending data via all these routes, the redundancy will ensure that all data arrives at the destination. An alternative mechanism to sending data via redundant routes is diversity coding.

All of these techniques have various degree of effectiveness. It widely acknowledged that cryptographic

techniques can provide the some of the strongest techniques to ensure the availability, integrity, and confidentiality of routing information.

This observations also holds true for many of the other MANET security problems highlighted in Figure 1.

4.2. Defining Key Management

Key management is the state where in networks node share keying material for use in cryptographic mechanisms. Keying materials include public/private key pairs, secret keys, initialization parameters, and non-secret parameters supporting key management in various instances. Key management have many techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. It includes following phase.

(i) Initialization of system users within a network.

(ii) Generation, Distribution, and installation of keying material.

(iii) Control over the use of keying material.

(iv) Update ,revocation, and destruction of keying material.

(v) Storage, backup/recovery, and archival of keying material.

(vi) Bootstrapping and maintenance of trust in keying material.

The fundamental function of key management schemes is the establishment of keying material. It is subdivided into key agreement and key transport. Both can be achieved using either symmetric or asymmetric techniques.

4.3. Requirements of Key Management Schemes

It includes the following generics services for security attributes:

Confidentiality. It should guarantee key secrecy, that is, ensure the inability of adversaries or unauthorized parties to study keying material.

Key authentication. Key authentication, in the context of a communication session between two parties, can either be unilateral or mutual: unilateral authentication means that only one party's keying material is authenticated, while mutual authentication involves validating both parties' keying material.

Key conformation. It is provided by a key establishment protocol, communication entities prove possession of authenticated keying material. Key authentication with key conformation yields explicit key authentication.

Key freshness. The key freshness features improves security by ensuring new and independent key between different communication sessions.

Resistant to known key attacks. It is vulnerable to known key attacks if a compromised past session key or subset of past session keys.

Perfect forward secrecy(PFS). Ensure that compromise of long terms key cannot result in compromise of past session keys.

Forwards secrecy. A key management scheme with a forward secrecy features prevents an adversary from discovering subsequent from a compromised contiguous subset of old keys.

Backward secrecy. A backward secrecy features prevents an adversary from discovering preceding keys from a compromised contiguous subset of old keys.

Key independence. Key independence guarantees that a passive adversary who knows a proper subset of keys cannot discover any other keys. Key independence supports both forward and backward secrecy. It does not imply key freshness.

Availability. A high-availability property prevents degradation of key management services and ensures that keying material is provided to nodes in the network when expected.

Robustness. The key management scheme have tolerated hardware and software failures, asymmetric and unidirectional links , and network partitioning/ fragmentation due to limited/ error phone wireless connectivity.

Resistance: capability of the system to defend against or tolerate attacks.

Recognition : capability of the system to detect attacks in process and monitor the extend of the damage and restore full services.

Recovery : the main feature of the survivability ; it is capability to maintain services during attack, limit the extent of the damage and restore full services.

Efficiency. The key management services should be efficient respect to communication, computational, memory, and energy resources.

Scalability. It ensures efficiency and availability as the number of networking nodes rapidly and significantly changes; the key management scheme should thus seamlessly scale to network size.

5. Peer-To-Peer Key Management For MANET

As mentioned in Section 1, the focus of this article is on peer-to-peer key management for mobile ad hoc networks (MANETs). Investigations by the authors within the available publications have led to the classification of the current protocols into the following subsets:

(1) Partially distributed certificate authority;
(2) Fully distributed certificate authority
(3) Identity-based key management;
(4) Certificate chaining-based key management;
(5) Cluster-based key management;
(6) Pre deployment-based key management;
(7) Mobility-based key management, and
(8) Parallel key management.

Most of the above subsets use public key cryptography due to its superiority in distributing keys, providing authentication, and achieving integrity and nonrepudiation. Symmetric key systems need a channel that provides both data integrity and confidentiality: the latter property may not always be readily available without any form of trusted authority or secure side channel (such as an infrared interface).

The partially distributed certificate authority group of protocols distributes the trust in the certificate authority to a subset of the network communication entities. The approach mitigates the single point of vulnerability inherent to the centralized certificate authority. Protocols considered to represent this implementation method were presented in Zhou and Haas [1999] and Yi and Kravets [2003], respectively. The fully distributed certificate authority protocol subset preserves the symmetric relationships between the communication entities in MANETs by distributing the burden of key management to all communication entities. Each authorized node in the network receives a share of the certificate authority's secret key, allowing neighbors to service requests for certification. The protocol that introduced this method was presented in Luo et al. [2002].

The identity-based key management approach borrows concepts from the partially distributed certificate authority protocols, but uses an identity-based cryptosystem to reduce the storage requirement compared to conventional public key cryptosystems. The protocol by Khalili et al. [2003] will be considered as representative of this protocol group.

In the certificate chaining-based key management approach, communication entities can authenticate certificates by means of finding certificate chains between them. Certificate chaining can be explained by the following example: party A wants to communicate with party C, which requires party A to authenticate party C's certificate.

The two parties have no communication history, but party A trusts the certificate of a third entity, party B. Party B informs party A that it trusts the certificate of party C. Party A that trusts party B will thus also trust party C as a result of party B's recommendation. There is thus a fully connected certificate chain between party A and C through party B, which enables party A to authenticate the certificate of party C without any previous communication.

The cluster-based key management subset relies on a clustering algorithm to subdivide the network into smaller groups. Group members in the same proximity can monitor their neighbors and make recommendations to members from other groups on the authenticity of their neighbors' certificates. The cluster-based subset is introduced by investigating the protocol presented in Ngai et al. [2004]. The pre-deployment-based key management subset makes use of an offline authority to issue each node with keying material prior to network formation. It is widely agreed that key pre-distribution techniques are ideally

suited for establishing secure connectivity in large-scale distributed sensor networks [Eschenauer and Gligor 2002].

The limitations of sensor networks render conventional key establishment techniques (such as public key cryptography).The mobility-based key management subset exploits mobility and node encounters to establish security associations and to warrant mutual authentication between users. In contrast to the previously discussed subsets, the protocols in this group introduce a shift in paradigm with respect to previous attempts to provide key management for fully self-organized MANETs. Rather than trying to adapt solutions suited for conventional wireline networks, the protocols in this subset use the unique characteristics of MANETs to their advantage.

The combination of any of the above key management approaches gives rise to what the authors call the parallel key management subset. By using two or more of the above approaches in parallel, the advantages of the one scheme is used to mitigate the disadvantages of the other. This subset can be represented by the scheme introduced in Yi and Kravets [2004], which combines a partially distributed certificate authority [Yi and Kravets 2003] and the certificate chaining- based key management approach [Capkun et al. 2003b].

6. Conclusion

Key management schemes based on the key pre distribution techniques proposed for sensor networks may be another avenue to solve the key management problem in authority-based MANETs. Another observation is related to the criteria used by researchers to analyze key management schemes for MANETs. Key management schemes are designed either for an ―open‖ (self-organized) or ―closed‖ (authority-based) network and consequently aimed at different applications―Open‖ or fully self-organized MANETs have some inherent security implications (such as being vulnerable against the Sybil attack) and must be analyzed accordingly. It is therefore not always possible to compare schemes that assume the existence of a trusted authority with those that are fully self-organized.

This study confirms that key management mechanisms proposed to guarantee the security of conventional networks are not necessarily suitable or adaptable to MANETs. Novel techniques, designed specifically for MANETs, are necessary. Key management is an important area that will need resolution before wide-scale deployment of ad hoc networks will become practical. Although key management for MANETs has reached a reasonable level of maturity, it is still a research area with room for innovation.

References

[1] A. Boldyreva, "Efficient Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme," Proc. Sixth Int'l Workshop Theory and Practice in Public Key Cryptography (PKC '03), pp. 31-46, 2003.

[2] B. Sonja and B. Jean-Yves Le, "Performance analysis of the confidant protocol," 2002, 513828 226-236.

[3] C. Blundo, A.D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. 12th Ann. Int'l Cryptology Conf. (CRYPTO '92), pp. 471-486, 1992.

[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (CRYPTO '01), pp. 213-229, 2001.

[5] D. B. Johnsort, "Routing in ad hoc networks of mobile hosts," in Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on, 1994, pp. 158–163.

[6] D. Hongmei, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol. 40, no. 10 70–75, 2002.

[7] Francis, M. Sangeetha, and A. Sabari, "A survey of key manage-ment technique for secure and reliable data transmission in manet," International Journal of Advanced Research in Computer Science and Software Engineering (IJAARCSSE), vol. 3, no. 1, pp. 22–27, 2013.

[8] G. Bracha, "An Asynchronous bðn _ 1Þ=3c-Resilient Consensus Protocol," Proc. Third Ann. ACM Symp. Principles of Distributed Computing (PODC '84), pp. 154-162, 1984.

[9] H. Yih-Chun, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 3, 2003, pp. 1976–1986 vol.3.

[10] J. J. Garcia-Luna-Aceves and M. Spohn, "Source-tree routing in wire-less networks," in Network Protocols, 1999. (ICNP '99) Proceedings. Seventh International Conference on, 1999, pp. 273–282.

[11] K. Barr and K. Asanovic, "Energy Aware Lossless Data Compression," Proc. First ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '03), pp. 231-244, 2003.

[12] K. Hussain, A. H. Abdullah, S. Iqbal, K. Awan, and F. Ahsan, "Efficient cluster head selection algorithm for manet," Journal of Computer Networks and Communications, vol. 2013, no. 7, pp. 1–7, 2013.

[13] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," Communications Surveys & Tutorials, IEEE, vol. 10, no. 4, pp. 78–93, 2008.

[14] L. Wenjing, L. Wei, and F. Yuguang, "Spread: enhancing data confiden-tiality in mobile ad hoc networks," in INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 4, 2004, pp. 2404–2413 vol.4.

[15] L. Lilien, "Developing pervasive trust paradigm for authentication and authorization," in Cracow Grid Workshop. Institute of Computer Science, AGH University of Science and Technology, Cracow,Poland: Academic Computer Centre CYFRONET AGH, 2004, pp. 42–49.

[16] M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security (CCS '93), pp. 62-73, 1993.

[17] M. Bellare, A. Boldyreva, and S. Micali, "Public-Key Encryption in a Multi-User Setting: Security Proofs and Improvements," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '00), pp. 259-274, 2000.

[18] M. Bellare, A. Boldyreva, and A. Palacio, "An Uninstantiable Random-Oracle-Model Scheme for a Hybrid Encryption Problem," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '04), pp. 171-188, 2004.

[19] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault Tolerant Distributed Computation," Proc. 20th Ann. ACM Symp. Theory of Computing (STOC '88), pp. 1-10, 1988.

[20] M. Sergio, T. J. Giuli, L. Kevin, and B. Mary, "Mitigating routing misbehavior in mobile ad hoc networks," 2000, 345955 255-265.

[21] O. Baudron, D. Pointcheval, and J. Stern, "Extended Notions of Security for Multicast Public Key Cryptosystems," Proc. 27th Int'l Colloquium on Automata, Languages and Programming (ICALP '00), pp. 499-511, 2000.

[22] P. Papadimitratos and Z. J. Haas, "Secure routing: Secure data transmis-sion in mobile ad hoc networks," in ACM Workshop on Wireless Security (WiSe 2003), vol. 1-58113-585-8/02/0009, San Diego, California, USA, 2003, pp. 41–50.

[23] P. Sivaprakasam and R. Gunavathi, "An efficient clusterhead election algorithm based on maximum weight for manet," in Advanced Com-puting (ICoAC), 2011 Third International Conference on, Dec 2011, pp315–320.

[24] R. Hauser, M. Consulting, T. Przygienda, and G. Tsudik, "Lowering security overhead in link state routing," Computer Networks, vol. 31, no. 8, pp. 885–894, 1999.

[25] S. Mehta, P. Sharma, and K. Kotecha, "A survey on various cluster head election algorithms for manet," in Engineering (NUiCONE), 2011 Nirma University International Conference on, Dec 2011, pp. 1–6.

[26] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE, vol. 3, 1997, pp. 1405–1413 vol.3.

[27] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," Communications Surveys & Tutorials, IEEE, vol. 8, no. 2, pp. 2–23, 2006.