IPHV7I20007X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SEMANTIC KEY PRE-DISTRIBUTION PROTOCOL FOR MULTI-PHASE WIRELESS SENSOR NETWORKS

#1KIRAN KUMAR BANDLA
#2Y.NAGENDRA KUMAR
Dept of CSE
SRI MITTAPALLI COLLEGE OF ENGINEERING, TUMMALAPALEM, GUNTUR, AP.

Abstract: **-** The problem of efficiently and securely broadcasting to a 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. In this paper, we circumvent these obstacles and close this gap by proposing a novel key management paradigm. The new paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any intended subgroup chosen in an *ad hoc* way. Following this model, we instantiate a scheme that is proven secure in the standard model. Even if all the non-intended members collude, they cannot extract any useful information from the transmitted messages. After the public group encryption key is extracted, both the computation overhead and the communication cost are independent of the group size. Furthermore, our scheme facilitates simple yet efficient member deletion/ addition and flexible rekeying strategies. Its strong security against collusion, its constant overhead, and its implementation friendliness without relying on a fully trusted authority render our protocol a very promising solution to many applications.

Keywords:- *Ad Hoc Network, Broadcast, Cooperative Computing, Key Management, Network Scalability.*

I.INTRODUCTION

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multihop backbone to connect to each other and Internet via long-range high-speed wireless techniques. The bottomlayer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. For instance, a manager on his way to holiday may want to send a confidential e-mail to some staff of her company via WMNs, so that the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, smartphones, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers. A MANET is a system made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an effective networking system facilitating data exchange between mobile devices even without fixed infrastructures. In MANETs, it is important to support group-oriented applications, such as audio/video

conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. In general, users working for the same mission form a cooperation domain; any particular application or interest in a network may lead to the establishment of a corresponding community. Since communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive information being intercepted by unintended recipients is a real concern. For instance, a commander may issue secret commands to soldiers in battlefield via satellite-to-MANET communication. Consequently, efforts to secure group communications in MANETs are essential.

II. RELATED WORK

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multihop backbone to connect to each other and Internet via
long-range high-speed wireless techniques. The bottomlayer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. For instance, a manager on his way to holiday may want to send a confidential e-mail to some staff of her company viaWMNs, so that the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, smartphones, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers. A MANET is a system made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an effective networking system facilitating data exchange between mobile devices even without fixed infrastructures. In MANETs, it is important to support group-oriented applications, such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. In general, users working for the same mission form a cooperation domain; any particular application or interest in a network may lead to the establishment of a corresponding community. Since communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive information being intercepted by unintended recipients is a real concern. For instance, a commander may issue secret commands to soldiers in battlefield via satellite-to-MANET communication. Consequently, efforts to secure group communications in MANETs are essential.

The major security concern in group-oriented communications with access control is key management. Existing key management systems in these scenarios are mainly implemented with two approaches referred to as group key agreement (or group key exchange by some authors) and key distribution systems (or the more powerful notion of broadcast encryption). Both are active research areas having generated large respective bodies of literature. Group key agreement allows a group of users to negotiate a common secret key via open insecure networks. Then, any member can encrypt any confidential message with the shared secret key and only the group members can decrypt. In this way, a confidential intra group broadcast channel can be established without relying on a centralized key server to generate and distribute secret keys to the potential members. A large number of group key agreement protocols have been proposed. The earlier efforts focused on efficient establishment of the initial group key. Later studies enable efficient member joins, but the cost for a member leave is still comparatively high. A tree key structure has been further proposed and improved to achieve better efficiency for member joins and leaves.The theoretical analysis in proves that for any tree-

based group key agreement scheme, the lower bound of the worst-case cost is rounds of interaction for member join or leave, where is the number of group members. This optimal round efficiency was recently achieved. By using a ring-based key structure, the up-to-date proposal in breaks this round barrier because only a constant number of rounds is required for member changes. In a key distribution system, a trusted and centralized key server presets and allocates the secret keys to potential users, such that only the privileged users can read the transmitted message. The early key distribution protocol does not support member addition/deletion after the system is deployed. This notion was subsequently evolved to allow the sender to freely choose the intended receiver subset of the initial group, which is usually referred to as broadcast encryption. Broadcast encryption is essential for key management in priced media distribution and digital rights management. Broadcast encryption schemes in the literature can be classified in two categories: symmetric-key broadcast encryption and public-key broadcast encryption. In the symmetric-key setting, only the trusted center generates all the secret keys and broadcasts messages to users. Hence, only the key generation center can be the broadcaster or the sender. In the public-key setting, in addition to the secret keys for each user, the trusted center also generates a public key for all the users so that any one can play the role of a broadcaster or sender. Fiat and Naor first formalized broadcast encryption in the symmetric-key setting and proposed a systematic method of broadcast encryption. Similarly to the group key agreement setting, tree-based key structures were subsequently proposed to improve efficiency in symmetric-key based broadcast encryption systems. The state of the art along this research line is presented, In the public-key setting, Naor and Pinkas presented in the first public-key broadcast encryption scheme in which up to a threshold of users can be revoked. If more than this threshold of users is revoked, the scheme will be insecure and hence not fully collusion-resistant. Subsequently, by exploiting newly developed bilinear paring technologies, a fully collusion-resistant public-key broadcast encryption scheme was presented that has complexity in key size, ciphertext size, and computation cost, where the maximum allowable number is of potential receivers. A recent scheme reduces the size of the key and the ciphertexts, although it has the same asymptotical sublinear complexity. An up-to-date scheme was presented in, which strengthens the security concept of public-key broadcast encryption schemes while keeping the same complexity.

B. Contribution

Our contribution includes three aspects. First, we formalize the problem of secure transmission to remote cooperative groups, in which the core is to establish a one-to-many channel securely and efficiently under certain constraints. We observe that the existing key management approaches do not provide effective solutions to this problem. On one hand, group key agreement provides an efficient solution to secure intragroup communication, but for a remote sender, it requires the sender to simultaneously stay online with the group members for multiple rounds of interactions to negotiate a common secret session key before transmitting any secret contents.

EXISTING METHOD:

Many security schemes developed for general network environments do not take into account the unique features of WSNs: Public key cryptography is not feasible computationally because of the severe limitations imposed on the physical memory and power consumption of the individual sensors. Traditional key exchange and distribution protocols are based on trusting third parties, and this makes them inadequate for large-scale WSNs whose topologies are unknown prior to deployment. *Random* key predistribution schemes were introduced to address some of these difficulties. The idea of randomly assigning secure keys to sensor nodes prior to network deployment was first introduced by Eschenauer and Gligor. The approach we use here considers random graph models naturally induced by a given scheme, and then develops models naturally induced by a given scheme, and then develops the scaling laws corresponding to desirable network properties, e.g., absence of secure nodes that are isolated, secure

IPHV7I20007X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

connectivity, etc. This is done with the aim of deriving guidelines to dimension the scheme, namely adjust its parameters so that these properties occur.

DISADVANTAGES:

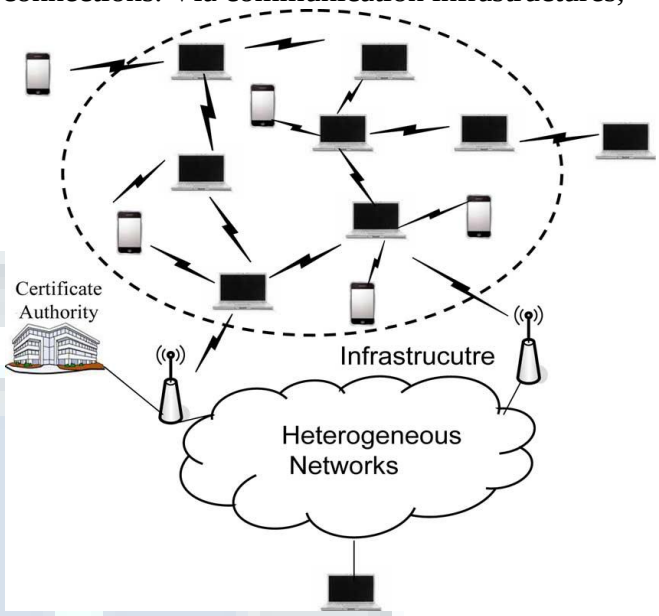
To be sure, the full-visibility assumption does away with the wireless nature of the communication medium supporting WSNs. In return, this simplification makes it possible to focus on how randomization in the key assignments alone affects the establishment of a secure network in the best of circumstances, i.e., when there are no link failures. A common criticism of this line of work is that by disregarding the unreliability of the wireless links, the resulting dimensioning guidelines are likely to be too optimistic: In practice, nodes will have fewer neighbors since some of the communication links may be impaired. As a result, the desired connectivity properties may not be achieved if dimensioning is done according to results derived under full visibility.

PROPOSED METHOD:

In this paper, in an attempt to go beyond full visibility, we revisit the pairwise key predistribution scheme of Chan *et al.* under more realistic assumptions that account for the possibility that communication links between nodes may not be available. This could occur due to the presence of physical barriers between nodes or because of harsh environmental conditions severely impairing transmission. To study such situations, we introduce a simple communication model where channels are mutually independent, and are either on or off. An overall system model is then constructed by *intersecting* the random graph model of the pairwise key distribution scheme (under full visibility).

III. IMPLEMENTATION

We address the above problem by formalizing a new key management paradigm referred to as group key agreement-based broadcast encryption. The system architecture is illustrated in Fig. 1. The potential receivers are connected together with efficient local connections. Via communication infrastructures,



they can also connect to heterogeneous networks. Each receiver has a public/secret key pair. The public key is certified by a certificate authority, but the secret key is kept only by the receiver.

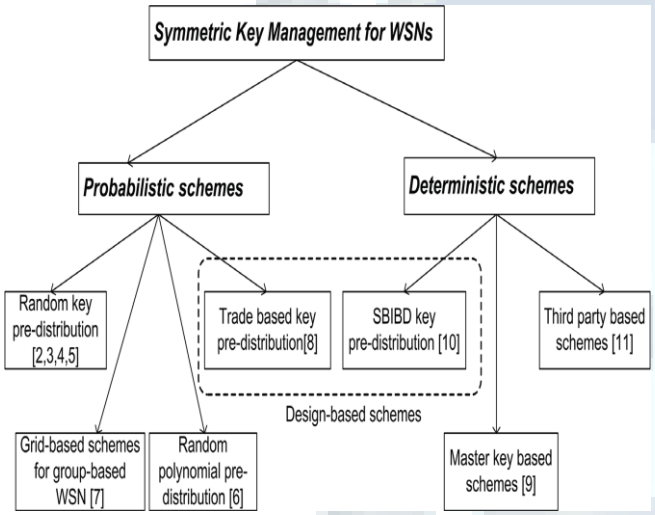
A remote sender can retrieve the receiver's public key from the certificate authority and validate the authenticity of the public key by checking its certificate, which implies that no direct communication from the receivers to the sender is necessary. Then the sender can send secret messages to any chosen subset of the receivers.

We next formally define the model of group key agreement- based broadcast encryption. The definition incorporates the up-to-date definitions of group key agreement and public-key broadcast encryption. Since the core of key management is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can simultaneously encrypt any message under the session key, and only the intended receivers can decrypt. Specifically, our key management system consists of the following (probabilistic) polynomial-time algorithms. Operator try to derive event attribute values they are by policy not allowed to access directly. We want to avoid that hosts maliciously or inadvertently obtain information from event streams for which they have no authorization. Note, by accessing event streams according to the specified system model,

IPHV7I20007X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

hosts may still be able to infer event attributes of unauthorized event streams from legally received event streams. An adversary in our system is therefore limited to the behavior described in the system model. The adversary is authenticated and can only access streams according to its properties. The derived event output follows the operator specification and the access require-ments for each executed operator. Each adversary is bound to analyzing outgoing event streams which it is allowed to access, for inferring any additional information.

IV.SYMMETRIC KEY MANAGEMENT



Key management problems in WSNs have been extensively studied in the literature and several solutions have been proposed . In this work, we mainly classify symmetric schemes into two categories: *probabilistic* schemes and *deterministic* ones (see Figure 1). In *deterministic* schemes, each two neighboring nodes are able to establish a direct secure link which ensures a total secure connectivity coverage. In *probabilistic* schemes, the secure connectivity is not guaranteed because it is conditioned by the existence of shared keys between neighboring nodes. We give in table I the definition of the five considered evaluation metrics, while we summarize in table II the main used symbols.

A. Probabilistic schemes

In probabilistic key management schemes, each two neighboring nodes can establish a secure link with some probability. If two neighboring nodes cannot establish a secure link, they establish a secure path composed of successive secure links. Eschenauer and Gligor proposed in the basic Random Key Pre-distribution scheme denoted by RKP. In this scheme, each node is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment step, each node i exchanges with each of its neighbor j the list of key identifiers that it maintains. This allows node j to identify the keys that it shares with node i. The values of the key ring size k and the key pool size $|S|$ are chosen in such a way that the intersection of two key rings is not empty with a high probability. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring. Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised. Chan *et al.* proposed in a protocol called Q-composite scheme that enhances the resilience of RKP. In this solution, two neighboring nodes can establish a secure link only if theyshare at least Q keys. The pairwise session key is calculated

TABLE

SUMMARY OF NOTATIONS

S The global key pool

$|S|$ The size of the global key pool

KRi The key ring of node i

$|KRi|$ The size of the node i key ring

n The network size (number of nodes)

l The key size

Q The minimum number of common keys required to establish a secure link in the Q-composite scheme

m The design order (SBIBD and Unital)

k Key ring size & Block size of a given design

(q, k) The two parameters of the Ruj *et al.* trade construction (k is also the block size) $p(i)$ The probability that two nodes share exactly I keys in their subset of keys Pc The probability that two nodes can establish a secure link Rx The network resiliency when x nodes are captured as the hash of all shared keys concatenated to each other:

$Ki,j = Hash(Ks1Ks2 \ldots\_Ksq)$ where $Ks1, Ks2, \ldots Ksq\_$ are the $q\_$ shared keys between the two nodes i and j ($q\_ \geqslant Q$).

This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link. However, this approach degrades the network secure connectivity coverage because neighboring nodes must have at least *Q* common keys to establish a secure link.

Chan *et al.* proposed also in a perfect secure pairwise key pre-distribution scheme where they assign to each possible link between two nodes *i* and *j* a distinct key *Ki,j*. Prior to deployment, each node is pre-loaded with $Pc \times n$ keys, where *n* is the network size and *Pc* is the desired secure coverage probability. Since we use distinct keys to secure each pairwise link, the resiliency against node capture is perfect and each captured node does not reveal any information about external links. The main drawback of this scheme is the non scalability because the number of the stored keys depends linearly on the network size.

VI.CONCLUSION

We proposed, in this work, a scalable key management scheme which ensures a good secure coverage of large scale WSN with a low key storage overhead and a good network resiliency. We make use of the unital design theory.

We proposed then an efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage. We discuss the solution parameter and we propose adequate values giving a very good trade-off between network scalability and secure connectivity. We conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances.

REFERENCES

[1] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh-" A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks"- IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013

[2] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 2002 ACM CCS*, pp. 41–47.

[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE SP*, pp. 197–213, 2003.

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. 2004 IEEE INFOCOM*, pp. 586–597.

[5] C. Castelluccia and A. Spognardi, "A robust key pre-distribution protocol for multi-phase wireless sensor networks," in *Proc. 2007 IEEE Securecom*, pp. 351–360.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. 2003 ACM CCS*, pp. 52–61.

[7] Z. Yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in *Proc. 2005 IEEE WCNC*, pp. 1915–1920.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs," in *Proc. 2011 IEEE INFOCOM*, pp. 326–330.

[9] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in *Proc. 2003 ACM CCS*,pp. 62–72.

[10] S. A. C¸ amtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 15, pp. 346–358, 2007.

[11] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "Spins: security protocols for sensor netowrks," in *Proc. 2001 ACM MOBICOM*,pp. 189–199.

[12] B. Maala, Y. Challal, and A. Bouabdallah, "Hero: hierarchcal key management protocol for heterogeneous WSN," in *Proc. 2008 IFIP WSAN*, pp. 125–136.

[13] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new scalable key predistribution scheme for WSN," in *Proc. 2012 IEEE ICCCN*, pp. 1–7.

[14] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *J. Netw. Comput. Appl.*, vol. 33, no. 2, pp. 63–75, 2010.

[15] S. A. C¸ amtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Technical Report TR-05-07, Mar. 2005.

AUTHORS DETAILS

[1] Kiran Kumar Bandla completed M.Sc(CS) from Bapatla engineering college, Bapatla in 2010. He is currently doing M.Tech (CS) from srimittapalli college of engineering ,tummalapalem,Guntur,AP.

[2] Y.NAGENDRA KUMAR , working as an Assistant professor in srimittapalli college of engineering. He received his M.Tech(CSE) from JNTUK.He completed his B.techfrom Sir C R Reddy College Of Engineering . His areas of interest are Cryptography and Network Security, Data warehousing and Data mining, Computer networks.