IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Study on Trusted Communication in Wireless Networks

S. Hemalatha

Department of Computer Applications, Idhaya College for Women, Kumbakonam, Tamilnadu, India

Corresponding Author: hemakeerthi313@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—** Several algorithms are proposed which uses the basic scheme by predistributing random keys into nodes. The drawback is that one pair wise key may be shared by multiple links. Chan et al. presented two schemes. In their q-composite scheme, multiple keys are required to establish a secure link, which makes a trade-off between connectivity and security. In their random pair wise-key scheme, a unique pair wise key is assigned to each node and every one of a random set. This scheme provides high security but poses an upper bound on network size. Du et al. proposed the pair wise key predistribution scheme based on both the basic scheme and Blom's scheme, from which it inherits the threshold property. On the contrary, our scheme utilizes Blom's scheme more smoothly.

***Keywords*—** Wireless, Authentication, Sensor network, Trust management

I. INTRODUCTION

Du et al. and Liu and Ning independently proposed to utilize deployment knowledge to improve the performance of key establishment. Our scheme outperforms Du's deployment knowledge scheme in terms of connectivity and security. Liu and Ning's polynomial-based key predistribution scheme also has the threshold property for the use of bivariate polynomials, which is a special form of Blom's scheme. As we mentioned, our scheme utilizes the deployment knowledge in a smoother way. Different from all of these, Zhu et al. presented LEAP by introducing a weaker model, which assumes that there exists a short time interval within which nodes can establish pair wise keys securely. However, this time interval is often very hard to estimate accurately. Once it is overestimated, all links may be compromised.

Probabilistic Key Sharing discussed most of the proposed symmetric key cryptography protocols for establishing a pair wise shared key between two nodes make use of an on-line key server. Mitchell and Piper proposed a solution based on probabilistic key sharing that does not depend on such an on-line server. However, the storage complexity imposed on each participant in their scheme seems to be unaffordable in the context of ad hoc networks.

The probabilistic keying scheme in our protocol is similar to schemes that have been used by other researchers. Eschenauer and Gligor introduced a key management scheme based on probabilistic key sharing for distributed sensor networks (DSN) with central key servers (e.g., base stations). Chan et al. extended this scheme by presenting three new mechanisms for key establishment in sensor networks based on the framework of probabilistic key predeployment, including a mechanism for pair wise shared key establishment called multipath key reinforcement. Our work differs from the previous ones in severalaspects.

First, in our scheme, a node can deduce the set of keys it shares with any other node (which may be an empty set) only based on the latter's identity. In contrast, the approaches require each node to exchange the ids of the keys it possesses with its neighbours. Thus, our approach trades computation for communication, which is desirable in ad hocnetworks.

Second, Eschenauer and Gligor proposed using the predeployed keys for encrypting all communication between nodes. A session key between two nodes can also be established using a logical path secured by the predeployed keys. However, it seems that the established session key might not be exclusively known to the two nodes involved, because each predeployed key is known to several nodes. In contrast, we propose using the predeployed keys for establishing a shared pair wise key that is exclusively known to two nodes with overwhelming probability.

II. THRESHOLD SECRET SHARING

There has been a great deal of research on threshold secret sharing Shamir and its applications. In one direction, Gong proposed an approach in which threshold secret sharing is used for increasing the availability of authentication services. Our work bears the similarity that we also utilize secret

sharing techniques to establish pair wise keys. Unlike Gong's scheme, however, our scheme does not use any single on-line key server. In another relevant direction, researchers have extensively investigated the interplay of network connectivity and secure and reliable communication (e.g., Dolev, Delev et al., Franklin and Wright, Desmedt and Wang). We refer the reader to Bagchi et al. For an overview and recent result in thisregard.

Network, Node and Security Assumptions First, we assume network links are bidirectional, i.e., if node A can hear node B, B can also hear A. This is true when all the nodes use omnidirectional antennas and have equal power levels.Second, we aim to provide solutions for low-end devices. The resources of a node such as power, storage, computation and communication capacity, are relatively constrained, making public key techniques impractical. We assume that every node has space for storing hundreds of bytes or a few kilobytes of keying materials, depending on the security requirements. Third, we do not assume a central key server exists in the formed network, whereas it may exist off-line to initiate the nodes prior to the formation of thenetwork. Fourth, we assume that if a node is compromised, all the information it holds will also be compromised. We do not distinguish between a compromised node and an attacker.

Moreover, all the compromised nodes may try to eavesdrop on other nodes' communications and collude to launch attacks by sharing their keying materials.provider invented the cloud computing. within a few years, emerging cloud computing has become the hottest technology.

III. KEY DISTRIBUTION

Our pair wise key establishment protocol is based on two techniques – probabilistic key sharing and threshold secret sharing. Before the deployment of a network, i.e., during a key pre-distribution phase, every node is loaded with a (small) fraction of keys out of a large pool of keys by a keyserver.

Note that this phase occurs before the deployment of the network, and the key server stays off-line after finishing this phase. Keys are allocated to each node using a probabilistic scheme that enables every pair of nodes to share one or more keys with certain probability. The keys directly shared between any two nodes can thus be used to encrypt messages exchanged between them. Even if two nodes do not share any keys directly, our probabilistic key sharing scheme enables them to communicate securely using logical paths obtained via a logical path discovery process[1].

To be concrete, consider two nodes u and v that wish to communicate privately. u and v may already share one or more keys from the pool of keys after the key predistribution phase. However, these keys are not known exclusively to u and v because every key in our key pool may be allocated to multiple nodes; hence, they cannot be used for encrypting any message that is private to u and v. Thus the goal of our algorithm is to establish a key, S, that is known exclusively to u and v. The basic idea underlying the establishment of such a key S is as follows: The sender node splits S into multiple shares using an appropriate secret sharing scheme. The sender then transmits to the recipient node all these shares, using a different logical path for each share. The recipient node then reconstructs S after it receives all (or a certain number of) the shares.

IV. SENSOR NODES

Sensor networks are ideal candidates for applications such as military target tracking, home security monitoring, and scientific exploration in dangerous environments. Typically, a sensor network consists of a potentially large number of resource constrained sensors, which are mainly used to collect data (e.g. temperature) from the environment, and a few control nodes, which may have more resources and may be used to control the sensors and/or connect the network to the outside world (e.g. a central data processingServer). Sensors usually communicate with each other through wireless communication channels. Sensor networks may be deployed in hostile environments, especially in military applications. In such situations, the sensors may be captured, and the data/control packets may be intercepted and/or modified. Therefore, security services such as authentication and encryption are essential to maintain the network operations. However, due to the resource constraints on the sensors, many security mechanisms such as public key cryptography are not feasible in sensor networks. Indeed, providing security services in sensor networks is by no means a trivial problem; it has received a lot of attention recently[1].

A fundamental security service is the establishment of a symmetric, pair wise key shared between two sensors, which is the basis of other security services such as encryption and authentication. Several key predistribution techniques have been developed recently to address this problem. Eschenauer and Gligor proposed the basic probabilistic key predistribution, in which each sensor is assigned a random subset of keys from a key pool before the deployment of the network. By doing this, two sensors can have a certain probability to share at least one key. Chan et al. developed the q-composite key predistribution and the random pair wise keys schemes. The q- composite key predistribution scheme is based on the basic probabilistic scheme, but it requires two sensors share at least q predistributed keys to establish a pair wise key. The random pair wise keys scheme pre distribute random pair wise keys between a particular sensor and a random subset of other sensors, and has the property that compromised sensors do not lead to the compromise of pair wise keys shared between non- compromised sensors.

However, these approaches still have some limitations. For the basic probabilistic and the q- composite key predistribution, a small number of compromised sensors may reveal a large fraction of pair wise keys shared between non-compromised sensors. Though the random pair wise keys scheme provides perfect security against node captures, the maximum supported network size is strictly limited by the storage capacity for pair wise keys and the desired probability to share a key between two sensors. Liu and Ning developed a framework to predistributepair wise keys using bivariate polynomials and proposed two efficient instantiations, a random subset assignment scheme and a grid- based key predistribution scheme, to establish pair wise keys in sensornetworks.

Our second theme during this paper is thought-about associate degree internal representation of this framework however can do higher performance thanks to the specific usage of location data. Recent advances in electronic and pc technologies have paved the manner for the proliferation of wireless detector networks (WSN). Detector networks typically comprises an oversized variety of ultra-small autonomous devices. every device, known as a detector node, is battery battery-powered and equipped with integrated sensors, processing capabilities, and short-range radio communications. In typical application eventualities, detector nodes square measure unfold every which way over the preparation region beneath scrutiny and collect detector information. samples of detector network comes embrace SmartDust and WINS.

Sensor networks ar being deployed for a large kind of applications, together with military sensing and pursuit, atmosphere observation, patient observation and pursuit, good environments, etc. once sensing element networks ar deployed during a hostile atmosphere, security becomes extraordinarily necessary, as they're vulnerable to differing kinds of malicious attacks. for instance, associate individual will simply hear the traffic, impersonate one in every of the network nodes1, or by choice give deceptive data to different nodes. to supply security, communication ought to be encrypted and echt. associate open analysis drawback is the way to bootstrap secure communications among sensing element nodes, i.e. the way to discovered secret keys among human activity nodes?

V. KEYMANAGEMENT

This key agreement drawback could be a a part of the key management drawback, that has been wide studied generally network environments. There ar 3 sorts of general key agreement themes: trusted-server scheme, self-enforcing theme, and key pre-distribution theme. The trusty-server theme depends on a trusted server for key agreement between nodes, e.g., Kerberos. this sort of theme isn't appropriate for detector networks as a result of there's typically no trusty infrastructure in detector networks. The self-enforcing theme depends on uneven cryptography, like key agreement mistreatment public key certificates. However, restricted computation and energy resources of detector nodes usually create it undesirable to use public key algorithms, like Diffie-Hellman key agreement or RSA, as realized. The third form of key agreement theme is vital pre-distribution, wherever key info is distributed among all detector nodes before preparation. If we all know that nodes ar additional seemingly to remain within the same neighbourhood before preparation, keys are often set a priori. However, attributable to the randomness of the preparation, knowing the set of neighbours deterministically may not be possible[5].

There exist variety of key pre-distribution schemes. A naive resolution is to let all the nodes carry a master secret key. Any try of nodes will use this international master secret key to attain key agreement and acquire a brand new try wise key. This theme doesn't exhibit fascinating network resilience: if one node is compromised, the protection of the complete detector network are compromised. Some existing studies counsel storing the key in tamper-resistant hardware to cut back the danger, however this will increase the price and energy consumption of every detector.what is more, tamper- resistant hardware won't perpetually be safe. Another key pre- distribution theme is to let every detector carry N − one secret try wise keys, every of that is thought solely to the present detector and one in all the opposite N−1 sensors (assuming N is that the total variety of sensors). The resilience of this theme is ideal as a result of compromising one node doesn't have an effect on the protection of communications among alternative nodes; but, this theme is impractical for sensors with a very restricted quantity of memory as a result of N may be massive. Moreover, adding new nodes to a pre-existing detector network is tough as a result of the prevailing nodes don't have the new nodes'keys.

The Eschenauer-Gligor theme has been delineated earlier during this section. we'll provides a additional elaborated description of this theme in Section II. supported the Eschenauer-Gligor theme, Chan, Perrig, and Song projected a q-composite random key pre-distribution theme. The distinction between this theme and therefore the Eschenauer-Gligor theme is that letter common keys (q nine 1), rather than simply one one, ar required to ascertain secure communications between a try of nodes. it's shown that, by increasing the worth of letter, network resilience against node capture is improved, i.e., associate offender needs to compromise more nodes to realize a high chance of compromised communication [3]. Du, Deng, Han, and Varshney projected a brand new key predistribution theme, that well improves the resilience of the network compared to the present schemes. This theme exhibits a pleasant threshold property: once the amount of compromised nodes is a smaller amount than the edge, the likelihood that any nodes apart from these compromised nodes ar affected is near zero. This

fascinating property lowers the initial payoff of smaller scale network breaches to AN soul, and makes it necessary for the soul to attack a big proportion of the network. an identical methodology is additionally developed by Liu andNing.

The ideas delineated during this paper is applied to all or any of the higher than pre-distribution schemes to additional improve their performance. Blundo et al. projected many schemes which permit any cluster of t parties to figure a typical key whereas being secure against collusion between a number of them. These schemes concentrate on saving communication prices whereas memory constraints aren't placed on cluster members. Perrig et al. projected SPINS, a security design specifically designed for detector networks. In SPINS, every detector node shares a secret key with the bottom station. 2 detector nodes cannot directly establish a secret key. However, they will use the bottom station as a sure third party to line up the key.

Several other key distribution schemes have been proposed for mobile computing, although they are not specifically targeted at sensor networks. Tatebayashi, Matsuzaki, and Newman consider key distribution for resource-starved devices in a mobile environment. This work is further improved by Park et al. Other key agreement and authentication protocols include the one by Beller and Yacobi. A survey on key distribution and authentication for resource-starved devices in mobile environments is given. The majority of these approaches rely on asymmetric cryptography, which is not a feasible solution for sensor networks. Several other methods based on asymmetric cryptography are also proposed: Zhou and Hass propose a secure ad hoc network using secret sharing and threshold cryptography. Kong et al. also propose localized public-key infrastructure mechanisms, based on secret sharing schemes.

VI. DISTRIBUTEDNETWORKS

Distributed sensor networks have received a lot of attention recently due to their wide application in military as well as civilian operations. Example applications include target tracking, scientific exploration, and monitoring of nuclear power plants. Sensor nodes are typically low-cost, battery powered, and highly resource constrained, and usually collaborates with each other to accomplish their tasks [1].

Security services such as authentication and key management are critical to secure the communication between sensors in hostile environments. As one of the most fundamental security services, pair wise key establishment enables the sensor nodes to communicate securely with each other using cryptographic techniques. However, due to the resource constraints on sensor nodes, it is not feasible for sensors to use traditional pair wise key establishment techniques such as public key cryptography and key distribution centre (KDC).

Eschenauer and Gligor proposed a probabilistic key predistribution scheme recently for pair wise key establishment. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment so any two sensor nodes have a certain probability of sharing at least one common key. Chan et al. further extended this idea and developed two key predistribution techniques: q-composite key predistribution and random pair wise keys scheme [6]. The q-composite key predistribution also uses a key pool but requires two sensors compute a pair wise key from at least q predistributed keys they share. The random pair wise keys scheme randomly picks pairs of sensors and assigns each pair a unique random key. Both schemes improve the security over the basic probabilistic key predistribution scheme. However, the pair wise key establishment problem is still not solved. For the basic probabilistic and the q-composite key predistribution schemes, as the number of compromised nodes increases, the fraction of affected pair wise keys increases quickly. As a result, a small number of compromised nodes may affect a large fraction of pairwise keys. While the random pair wise keys scheme doesn’t suffer from the above security problem, given a memory constraint, the network size is strictly limited by the desired probability that two sensors share a pair wise key and the number of neighbour nodes that a sensor can communicate withit.

VII. RELATEDWORKS

Some general key distribution and management approaches aren't appropriate for wireless sensing element networks. First, trivially storing in every node a combine wise key for each different node poses a high memory demand unaffordable for sensing element nodes. Second, on-line key distribution and management offered by the bottom station is inefficient for wireless sensing element networks owing to high communication overhead. Third, public-key algorithms like RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) square measure too high-ticket to current sensing element nodes for prime energy consumption and computation overhead. Experimental results from existing analysis show that the execution time of public key-primarily based operations, like cryptography and cryptography, is of the order of seconds or perhaps ten seconds. Moreover, wireless sensing element networks might not be able to offer the specified public-key infrastructure (PKI) for key distribution. we've to either distribute public keys into nodes through the bottom station on-line, which can cause high communication overhead, or predistribute public keys into nodes offline, which can want some theme like what we have a tendency to gift during this paper to boost itspotency.

Fortunately, the bootstrapping problem can be solved by key predistribution schemes that predistribute secret information in nodes to help them establish secure links after deployment.

Eschenauer and Gligor proposed basic scheme by utilizing probabilistic key predistribution, which was improved byChanet al. And Duet al. Recently, Duet al.And Liu and Ning independently proposed to make use of deployment knowledge to further improve the performance of key establishment. Different from all these schemes, LEAP proposed by Zhu et al. assumes a weaker model, that is, there exists a short time interval within which nodes can establish pair wise keys safely after deployment.

XI. PREDISTRIBIUTIONSCHEME

Group-based preparation information implies that every cluster of nodes reside solely among alittle native space, which implies that almost all of the neighbours of every node come back from its own cluster and neighbour teams. Therefore, to attain a extremely connected network, the key purpose is to maximise the likelihood that nodes from identical cluster and neighbour teams share keys. For this purpose, we have a tendency to divide the links of detector networks into 2 sorts, in-group links and intergroup links, reckoning on whether or not the concerned nodes area unit from identical cluster or not, severally. consequently, we have a tendency to build 2 styles of secret matrices A and B, severally [8]. Our theme consists of key predistribution part and key discovery part. Key Predistribution Phase: during this part, we have a tendency to generate a worldwide public matrix G and variety of secret A and B matrices. All teams share the world matrix G, which implies each node of a gaggle can choose a corresponding column from G. Meanwhile, every cluster is assigned a singular secret matrix A, that is, each node of {a cluster|agaggle|a bunch} can choose its corresponding row from the distinctive matrix A assigned to its group. Thus, we have a tendency to guarantee that any 2 nodes from identical cluster will forever notice a combine wise key[10].

Then, we tend to assign every cluster some variety of B matrices to ensure that every combine of neighbour teams shares a minimum of one common matrix B. a lot of exactly, we tend to 1st choose some teams and assign every of them a unique secret matrix B, wherever these teams are known as basic teams, and that we decision alternative nonbasic teams traditional teams. Then, for every cluster (including basic and traditional groups), we tend to assign it all of the B matrices that are allotted to its neighbour basic teams, that ar the essential teams among its neighbour teams. After that, every node picks corresponding rows from some or all (depending on totally different methods) of the B matrices that are allotted to its cluster. At last, we tend to set all nodes an equivalent transmission vary and deploy them in teams.

X. CONCLUSIONS

After deployment, each node first probes its neighbours. Then, neighbour nodes exchange their group indexes, indexes of B matrices, and columns of matrix G. If two neighbours come from the same group, they derive the pair wise key from the common matrix A and G. If they are not from the same group, but share one or more common B matrices, they can also find out the pair wise key from one shared matrix B and the global matrix G. Then, the neighbours with pair wise keys established will build a secure link between each other and start to transmit data securely through the link. Meanwhile, those neighbours sharing no pair wise keys will no longer communicate with each other. Note: Some nodes that find no pair wise keys between them may still exploit other methods such as multihop path reinforcement to establish pair wise keys indirectly. However, this discussion is out of the scope of our paper and we only focus on how to establish pair wise keys through one-hoplinks.

REFERENCES

[1] H.DaiandH.Xu,–Triangle-basedkeymanagement scheme for wireless sensor networks," Frontiers Electrical Electron. Eng. China, vol. 4, no. 3, pp. 300-306,2009.

[2] A.PoornimaandB.Amberker,–Tree-basedkey management scheme for heterogeneous sensor networks," in 16th IEEE International Conf. Netw.,2008.

[3] Y.Zhang,W.Yang,K.Kim,andM.Park,—AnAVLtree- based dynamic key management in hierarchical wireless sensor network," in Proc. International Conf. Intelligent Inf. Hiding Multimedia Signal Process., pp. 298-303,2008.

[4] A.PoornimaandB.Amberker,–Keymanagement schemes for secure communication in heterogeneous sensor networks," International J. Recent Trends Eng.,2009.

[5] A. Das, —An unconditionally secure key management scheme for largescale heterogeneous wireless sensor networks," in Proc. First International Commun. Syst. Netw. Workshops, pp. 1-10,2009.

[6] Y.Yang,J.Zhou,R.Deng,andF.Bao,–Hierarchicalself- healing key distribution for heterogeneous wireless sensor networks," SecurityPrivacyCommun.Netw., pp. 285-295, 2009.

[7] B. Tian, S. Han, and T. Dillon, —A key management scheme for heterogeneous sensor networks using keyed-hash chain," in 5th International Conf. Mobile Ad-hoc Sensor Netw.,2010.

[8] J.Kim,J.Lee,andK.Rim,–Energyefficientkey management protocol in wireless sensor networks," International J. Security its Appl.,2010.

[9] M.Wen,Z.Yin,Y.Long,andY.Wang,—Anadaptivekey management framework for the wireless mesh and sensor networks," Wireless Sensor Netw.J.,2010.

[10] H.Jen-Yan,I.Liao,andH.Tang,–Aforward authentication key management scheme for heterogeneous sensor networks," EURASIP J. Wireless Commun.Netw., 2010.

