SECURING CLUSTER BASED ADHOC NETWORK THROUGH BALANCED CLUSTERING WITH DISTRIBUTION AUTHORITIES OF KEY DISTRIBUTION AND KEY MANAGEMENT USING DEPLOYMENT KNOWLEDGE

Priyanka Manhas[1], Parminder Kaur[2]

[1]*Student,* [2]*Asst Prof, Department of Computer Science & Engineering, Chandigarh University (Gharuan, Mohali) India*
priyankamanhas36@gmail.com, parminder.cu@gmail.com

Abstract

In this paper, we address key management in cluster-based mobile ad hoc networks (MANETs). We present a fully-distributed ID-based multiple secrets key management scheme (IMKM). This scheme is implemented via a combination of ID-based multiple secrets and threshold cryptography. Ensuring secure communication in an ad hoc network is extremely challenging because of the dynamic nature of the network and the lack of centralized management. Our proposed analysis includes the effect of packet generation model, random deployment of sensors, dynamic cluster head assignment, data compression, and energy consumption model at the sensors. a new protocol called Equalized Cluster Head Election Routing Protocol (ECHERP), which pursues energy conservation through balanced clustering, is proposed. Performance evaluation of ECHERP is carried out through simulation tests. We also present a novel key predistribution scheme that uses deployment knowledge to divide deployment regions into overlapping clusters, each of which has its own distinct key space. Through careful construction of these clusters, network resilience is improved, we focus on the management of encryption keys in large-scale clustered WSNs. We propose a novel distributed key management scheme based on Exclusion Basis Systems (EBS); a combinatorial formulation of the group key management problem. Initially, clusters are formed in the network and the cluster heads are selected based on the energy cost, coverage and processing capacity. The sink assigns cluster key to every cluster and an EBS key set to every cluster head. The EBS key set contains the pairwise keys for intra-cluster and inter-cluster communication. During data transmission towards the sink, the data is made to pass through two phases of encryption thus ensuring security in the network. Our results include performance evaluation in terms of security metrics in clustered WSN and a detailed analysis of resource utilization.

Keywords: *cluster, deployment knowledge, energy efficiency key predistribution, event-driven, exclusion basis systems, hierarchical routing, ID-based cryptography, key agreement, key management, lifetime, location-aware protocols, mobile ad hoc network, Network coding, , random deployment, Security, secret sharing, secret key distribution, sensor networks, volatile environments, Wireless sensor networks secure group communications.*

----------***----------

1. INTRODUCTION

Recent literatures have sought to address the key management issues in MANETs. AD hoc networks are subject to various types of attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Moreover, it is difficult to deploy security mechanisms in MANETs because of the absence of fixed infrastructure, shared wireless medium, node mobility, limited resources of mobile devices, bandwidth restricted and error-prone communication links. Group key agreement (GKA) [3]-[4] is another important challenge of key management in MANETs. GKA protocols allow two or more parties to agree on a common group key and exchange information among them over an insecure channel. we propose an ID-based multiple secrets key management (IMKM) protocol to address all the above concerns. Our scheme is a comprehensive solution for inter and intra-cluster key Management, including key revocation, key update, and group key agreements. The main focus of this work is on the lifetime analysis of randomly deployed clustered networks. Clustered WSNs are suggested for extending the network scalability and ease of data processing, [1], [2]. In clustered networks, usually a representing node, called cluster head (CH), is assigned to each cluster. the lifetime of a randomly deployed clustered network is modeled using a probabilistic approach. The

probabilistic approach is motivated by the stochastic nature of the network lifetime which is mainly due to the randomness of the sensors deployment. Most of the protocols use clusters in order to provide energy efficiency and to extend the network lifetime. Each cluster first elects a node as the cluster head (CH), and then, the nodes in every cluster send their data to their own cluster head. The cluster head sends its data to the base station. This data transfer can be performed in two alternative ways. Either directly, in the case in which the cluster head is located close to the base station, or via intermediate cluster heads. In this paper, a novel energy efficient protocol, named ECHERP, is proposed. ECHERP, contrary to other existing cluster-based protocols that select a random node or the node with the higher energy at a particular time instance as the new cluster head, considers the current and the estimated future residual energy of the nodes, along with the number of rounds that can be cluster heads, in order to maximize the network lifetime. The network is modeled as a linear system. In this paper, we propose a novel key predistribution scheme that makes use of region-based deployment knowledge. Our scheme constructs a set of clusters such that each cluster contains a small number of deployment regions, all of which are neighbors of each other. Furthermore, every pair of neighboring deployment regions belongs to at least one cluster. Each cluster has its own distinct key space, and it is from these cluster key spaces that nodes are assigned their keys. In this manner, we guarantee that nodes in neighboring regions share a key with a given overlap probability, while nodes in non neighboring regions do not share any keys. We make use of the result developed in [18], which states that under certain conditions, maximizing the key pool size used by the scheme also maximizes its resilience. Our clustering scheme is designed to maximize the overall key pool size, which results in greatly improved network resilience without compromising network connectivity or communications overhead. Confidentiality, authenticity, availability, and integrity are typical security goals for WSNs. Indeed, securing the network for applications, such as border control and tactical defense operations is among the main design objectives. An EBS consists of several subsets of the member set collection. In the EBS, every subset is analogous to a particular key and the nodes which possess the key become the element of the subset.

The remainder of the paper is organized as follows: section 2 provide an (fully-distributed ID-based multiple secrets key management scheme) IMKM protocol. in section 3,we introduce proposed protocol that models the network as a linear system in order to select the cluster head that minimizes the energy consumption in the cluster, while in section 4,we present our basic predistribution scheme with EBS, In the EBS, every subset is analogous to a particular key and the nodes which possess the key become the element of the subset. Finally, we provide a conclusion with future directions in section 5.

2. IMKM (ID-BASED MULTIPLE SECRETS KEY MANAGEMENT SCHEME)

PROTOCLOS: This section presents our IMKM protocol. It consists of five phases: network initialization, key revocation, multiple secrets key update, member joining and eviction, and group key generation.

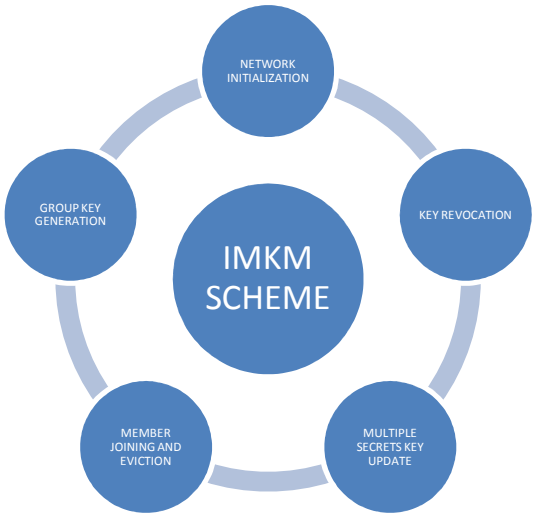

Fig 1 IMKM Protocol Phases

2.1 Network Initialization

Network initialization comprise in 3 steps. these are shown as below:

Fig 2 network initialization steps

The description of network initialization steps that is generation of pairing parameters and key initiation followed by generation of pair-wise keys with verifiable secret sharing is We consider basic operations in the scenario where there is an offline PKG center. These basic operations consist of system setup and private key extraction. system setup and key extraction is done in generation of pairing parameters and key initiation. A pair-wise key agreement protocol allows two parties to establish their session keys and use the keys to encrypt the communications between them. McCullagh and Barreto [31] proposed a two-party authenticated identity-based key agreement using bilinear pairings. In order to provide perfect forward secrecy, we modified their scheme to generate

our pair-wise keys. pair-wise key agreement protocol satisfies all the following security properties [31]: implicit key authentication, known session key security, no key-compromise impersonation, perfect forward secrecy, no unknown key-share and no key control. Therefore, it can be securely employed in MANETs. This is done in generation of pair-wise keys. And in verifiable secret sharing, In order to establish a (□, □) threshold sharing, we require that all cluster heads (CHs) participate in the construction of the master secret key, and that the role of distributed PKG (D-PKG) be assigned to the CHs of the network

2.2 Key Revocation

The key revocation scheme [34]-[36] is comprised of three sub-processes: misbehavior notification, revocation generation and revocation verification.

Fig 3 key revocation steps

2.2.1 Misbehavior Notification

Upon detection of CHi's misbehavior, CHj generates an accusation, $\{IDi, Tj\}Kj,v$, against CHi and securely transmits it to CHv , where Tj is a time stamp used to withstand message replay attacks and Kj,v is the pair-wise key of CHj and $CHv(1 \leq v \leq n, v \neq i, j)$. To prevent CHi from temporarily behaving normally (artificially), the accusation should not be sent to that node.

2.2.2 Revocation Generation

Upon receipt of an accusation from CH_j , the message will simply be dropped if the accuser itself has been revoked. The accused CH_i is diagnosed as compromised when the number of accusations against it reaches a predefined revocation threshold, β. In IMKM, generation of a revocation requires the joint effort of t CHs. We assume the D-PKG with the largest ID acts as the role of revocation leader. Each of the t unrevoked CH_j , having the smallest IDs, generates a partial revocation, $REV_j = H_1(ID_i)d_j$, and sends it to the revocation leader securely using the pair-wise key. The revocation leader checks whether the equation $H_2(P_{pub})REV_j = d_{jpub}H_1(ID_i)$ holds. If the partial revocation is not valid, the revocation leader considers CH_j to be misbehaving and issues a signed accusation against it. The revocation leader can construct a complete revocation from these partials using Lagrange interpolation. A complete revocation is derived as follows: $ID_i = \Sigma_{j\in\varepsilon}\ \lambda_j(0)REV_j = H_1(ID_i)D$. The revocation leader then floods $< ID_i, ID_i >$ throughout the network to inform others that CH_i has been compromised.

2.2.3 Revocation Verification

Upon receipt of $ID\ \ i$, each cluster head verifies it by checking whether the equation $H2(Ppub)ID\ i = H1(IDi)Dpub$ holds, where $Dpub$ can be computed using the public keys of the shares of any t unrevoked CHs. If the equation holds, this means that $ID\ '\ i$ has been correctly accumulated from all other $t-1$ unrevoked CHs. The cluster head then records IDi in its key revocation list (KRL) and declines to interact with it thereafter.

2.2.4 Multiple Secrets Key Update Scheme

In IMKM, all CHs' private keys, Sj , will last for the entire lifetime of the network, while the share keys, dj , used to enable key revocation and key update, are refreshed periodically for U predefined regular phases, using a multiple secrets key update scheme. Alternatively, they may be refreshed in key eviction process when the number of revocation CHs has reached a prescribed update threshold, γ. In this way, key update is quite simple and efficient because there is no need to exchange and sign any messages between the CHs.

2.3 Key Joining

In this section we show how to add a new cluster head, CHk, to the ad hoc network backbone.

2.4 Key Eviction

A cluster head eviction can happen as a result of unavailability, communication failure or for security reasons, such as revoked node. If the eviction of a CH is not considered a security vulnerability, such as a power failure, then no action is required. By using distributed key management schemes, each CH can easily add or update its share key in a secure and efficient manner, thus greatly reducing communication and computation costs.

2.5 Group Key Agreement Protocol

In this section, we present an efficient, one round authenticated group key agreement protocol (AGKA) for cluster-based MANETs. We may use the multiple secrets key update scheme.

2.6 Securing D-PKGs against DoS attacks

It has been suggested that wireless networks are highly susceptible to malicious denial-of-service (DoS) attacks, which prevent legitimate users from accessing the network. One such target is the key management service. Proper authentication can prevent injected messages from being accepted by the network. The key eviction procedure in our scheme is expected to be initiated very rarely. Therefore, if a malicious node were to frequently initiate this procedure in a short time window, then such an abnormality would be detected very easily. The legitimate nodes would then record the malicious node's ID in their key revocation lists and thereafter decline to interact with it.

3. PROPOSED PROTOCOL THAT MODELS THE NETWORK AS A LINEAR SYSTEM

The main characteristic of ECHERP is the head selection process. In this protocol, in order to elect a cluster head, the routing information and the energy spent in the network are formulated as a linear system, the solution of which is computed using the Gaussian elimination algorithm. Therefore, cluster heads are elected as the nodes that minimize the total energy consumption in the cluster. In most of the protocols proposed so far, the node with the highest residual energy in a cluster is elected as the cluster head. This selection may lead to inefficiencies, as can be seen by the following example. Let us assume that node x in Figure has higher residual energy than the other nodes belonging to the same cluster. Then, this node is elected as the new cluster head. However, this forces the rest of the nodes to send data in the opposite direction to the base station, resulting in higher energy consumption. In ECHERP, the BS is assumed to have unlimited energy residues and communication power. It is also assumed that the BS is located at a fixed position, either inside or away from the sensor field. The longer the distance between the BS and the center of the sensor field, the higher the energy expenditure for every node transmitting to the BS. All the network nodes, which are assumed to be located ithin the sensor field, are dynamically grouped into clusters. One of the nodes within every cluster is elected to be the cluster head of this cluster. Therefore, the number of cluster heads is equal to the number of clusters. The cluster heads, which are located close enough to the network base station, are referred to as the first level cluster heads. These cluster heads are capable of direct transmission to the base station with reasonable energy expenditure. The cluster heads that are located at more distant positions from the base station are considered as second-, third-, etc. level cluster heads. These cluster heads transmit data to the upper level cluster heads. Moreover, in order to achieve balanced energy consumption and extend the network's lifetime, the election of the cluster heads is performed in turns.

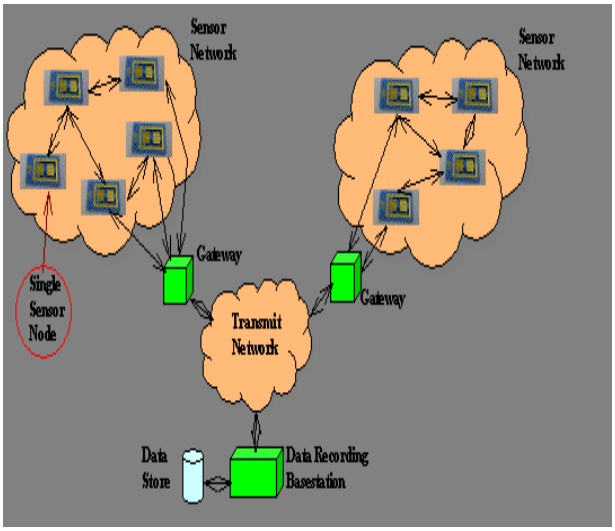

Fig 4 WSN network model

Obviously, this is not an energy efficient process, and it can be avoided by selecting cluster heads in a more energy efficient manner. This is pursued by the proposed protocol.

In order to evaluate the performance of ECHERP simulations, over 50 different 100 m × 100 m network topologies were performed. The network architecture considered is the following:

- A fixed base station is located away from the sensor field.
- The sensor nodes are energy constrained with uniform initial energy allocation.
- Each node senses the environment at a fixed rate and always has data to send to the base station (data are sent if an event occurs).
- The sensor nodes are assumed to be immobile. However, the protocol can also support node mobility.
- The network is homogeneous, and all the nodes are equivalent, i.e., they have the same computing and communication capacity.
- The network is location unaware, i.e., the physical location of nodes is not known in advance.
- The transmitter can adjust its amplifier power based on the transmission distance.

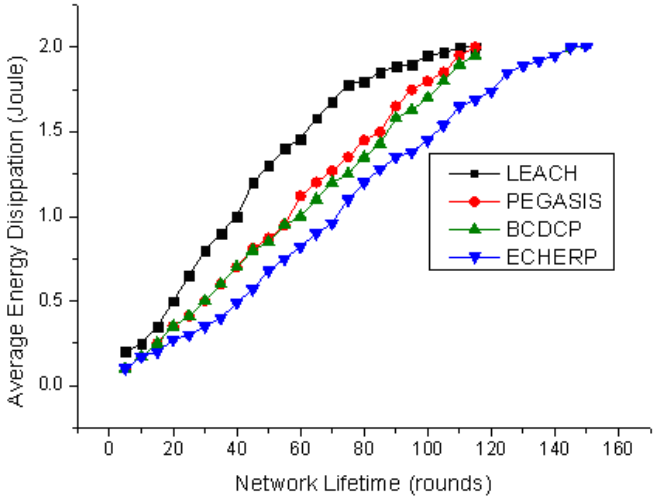

Fig 5 Network life time versus average energy dissipation

4. BASIC PREDISTRIBUTION SCHEME WITH EBS

There are 8 basic key distribution schemes that is described in tabular form with its different steps and complete description in front of one another. The basic 8 key pre-distribution scheme is RANDOM KEY PRE-DISTRIBUTION SCHEME, Q-COMPOSITE RANDOM KEY DISTRIBUTION SCHEMES, MULTIPATH KEY REINFORCEMENT SCHEME, Random pair wise key scheme, Polynomial pool-based key predistribution. Random subset key predistribution, Polynomial pool-based key predistribution, Random subset key predistribution, Grid based key predistribution, Hypercube key distribution scheme.

1. Random key predistribution scheme (proposed by Echenauer and Gligor). This is basic scheme[1].	➢ Key predistribution stage	➢ Large key pool of S keys and their identifiers are generated. From this key pool, k keys are randomly drawn and pre-distributed in to each node's keyring, including the identifiers of all those keys
	➢ Shared key discovery stage	➢ When the keys are initialized with keys, they are deployed in the respective places where they are needed. After deployment each node tries to discover its neighbors with which it share common keys.
	➢ Path key establishment stage	➢ A link exist between two nodes only if they share a key, but the path key establishment stage facilitates provision of the link between two nodes when they do not share a common key.
	➢ Key revocation	➢ Key revocation is conducted by the controller node, when a node is revoked then all the keys in that particular node keyring have to be deleted from the network.
	➢ Anayses of basic scheme	➢ Assume probability of a common key existing between two nodes in the network is p, and size of the network is n. then degree of the node is derivable using both p and n.
2. Q composite random key predistribution scheme[2] (proposed by Chan,perrigand song)	➢ As in basic scheme 2 nodes share a unique key for establishing a secure communication link and in Q composite random key predistribution scheme does this by requiring that two nodes have atleast q common keys to set up a alink.	➢ As amount of key overlap between two nodes is increased, it become harder for an adversary to break their communication link. To maintain the probability that two nodes establish a link with q common keys, it is necessary to reduce the size of key pool.
3. Multipath key reinforcement	➢ It offers good security with	➢ To solve the problem, the communication

scheme[2-10]	additional a communication overhead for use where security is more of a concern than bandwidth or power drain. ➢ The links formed between nodes after the key discovery phase in the basic scheme are not totally secure due to the random selection of keys from the key pool allowing nodes in a network to share some of the same keys and thereby possibly threaten multiple nodes when only one is compromised.	key between the nodes must be updated when one is compromised once a secure link is formed. ➢ This should not done for already established link, but should be coordinate during multiple independent paths for greater security.
4. Random pairwise key scheme[11]	➢ Compared to the Q-composite scheme and multipath scheme, the random pair wise scheme offers best security features in its resilience to node capture .	➢ The drawback of the random pair wise key scheme is lack of **scalability.**
5. Polynomial pool-based key predistribution[3] (proposed by liu and Ning)	➢ Any two sensors can definitely establish a pair wise key when there are no compromised sensors. ➢ Even with some nodes compromised, the others in the network can still establish pair wise keys. A node van find the common keys to determine whether or not it can establish a pair wise key and thereby help reduce communication overhead.	➢ Polynomial pool based key pre-distribution using random subsets offers greater security and flexibility when compared to other schemes until a certain number of compromised nodes assume 65% has been reached at which point at any scheme would prove ineffective. ➢ Advantages: Sensors can be added dynamically without consulting the already deployed sensors while dynamically deploying nodes in random pair wise demands that the server has pre designated un assigned space for additional nodes which may never be deployed.
6. Random subset key predistribution[1-3]	➢ This is an extension of the polynomial pool based scheme using a random subset key assignment and the basic scheme. ➢ In this the pair wise keys generated by each node are unique and based upon each node's ID. ➢ Random subset scheme works similar to the polynomial pool	➢ In key predistribution stage, the setup server generates a set F of S-bivariate t-degree polynomial and then initialize each node with a subset of s polynomials from F. ➢ In key discovery stage, each node attempt to determine the nodes with which they share a common key by employing the real time discovery techniques information is not preloaded in the nodes prior to the deployment . ➢ In path key establishment phase, a source node sends a message to its intermediate

	base4d scheme in three stages of key establishment. If no more than t shares of the same polynomial have been disclosed, it is very difficult to attack the communication between two nodes	nodes seeking to establish a connection with a destination node and if an intermediate node can share a common key with both the source and destination node, then the communication path is formed between the two.
7. Grid based key predistribution[3]	➢ A polynomial pool based scheme using a grid based key assignment offers all the attractive properties of the polynomial pool based key predistribution and guarantees that two sensor can establish a pair wise key, when there are no compromised nodes and the nodes can communicate with each other.	➢ Even if some nodes are captured , there will still be a great chance for key establishment between uncompromised nodes using this approach, which also reduce network communication overhead.
8. Hypercube keydistribution scheme[19]	➢ Guarantees that any two nodes in the network can establish a pair wise key if there are no compromised nodes are present as long as the two nodes can communicate.	➢ If two nodes cannot share the common polynomial, then they have to use the path discovery method to compute an indirect key. It include: dynamic path discovery, performance and overhead for the hypercube scheme, security evaluation for hypercube scheme.

	M1	M2	M3	M4	M5	M6	M7	M8	M9
K1	0	0	0	0	1	1	1	1	1
K2	0	1	1	1	0	0	0	1	1
K3	1	0	1	1	0	1	1	0	1
K4	1	1	0	1	1	0	1	0	0
K5	1	1	1	0	1	1	0	1	0

Fig 6 EBS matrix

THESE are all key predistribution schemes and in EBS it can be stated as:

4.1 EBS Construction

An EBS consists of several subsets of the member set collection. In the EBS, every subset isanalogous to a particular key and the nodes which possess the key become the element of the subset.The dimension of the EBS is represented by (N, K, M) and it depicts a condition of a N membered secure group with numbering from 1 to N and a separate key is maintained for every subset by the key server. In EBS, if there exists a subset Ai, then every member of this subset will have knowledge about the key Ki. In EMS, there are M elements for every t € [1, N] and its union is equal to [1, N] – {t}. Hence, any member t can be ejected by the key server. Then re-keying is performed to enable every member to know the replacement keys for the K keys. To perform this, the M messages are multicast after encrypting them with the keys which correspond to the M elements, which has a union equal to [1, N] – {t}. To restrict decipherability to selected

members, encryption of every key is performed by its predecessor.A canonical enumeration technique is made use of, for the construction of EBS subsets. In theformation of subset of K objects out of K + M object set, every feasible method is taken into consideration. Matrix A is formed in order to develop a bit string sequence in its canonical (K, M), in which the K and M are already known, C (K + M, K) columns indicate the successive bit strings of which has a length of K+M objects, where K ones are present in each. For EBS (N, K, M), "A" is known as the canonical matrix. For instance, the canonical matrix can be shown as:

1) No. of columns is equal to no. of nodes in the cluster.
2) No. of rows is equal to no. of keys used to manage these nodes.
3) Total no. of keys K+M.
4) Out of Size of EBS depend upon no. of nodes and no. of keys used to manage these nodes.
5) k+m keys,every sensor node know a distinct set of K keys that is set of keys known to one of sensor nodes can not be exactly identical to the set known to other sensor nodes.
6) No. of nodes = (K+M)!/K!M!
7) Value of K and M adjusted according to network and its security requirements

CONCLUSIONS WITH FUTURE DIRECTIONS

We have proposed a secure, efficient, and scalable distributed ID-based multiple secrets key management scheme (IMKM) for cluster-based mobile ad hoc networks. In order to address the highly dynamic topologies and varying link qualities of ad hoc networks, the master secret key is generated and distributed by all clusterheads. As a result, not only are central instances avoided, which constitute single points of attack and failure, but this also leads to more autonomous and flexible key update methods. According to our protocol analysis, we believe that the proposed IMKM scheme improves on the security and performance of previously proposed key management protocols. After the key distribution, secure channel is established between the nodes and the cluster head. During the data transmission from the cluster members to the sink, the data passes two phases. In the first phase the data is encrypted and transmitted to the cluster head. In the second phase, the data is encrypted by another key by the cluster head and then transmitted to the sink. Thus this technique allows inter cluster as well as intra cluster communication in a very efficient manner with high security. The sink then provides the cluster head with the cluster key and the EBS key set required for the communication between the nodes. These keys are distributed to the nodes by the cluster head prior communication. ECHERP, an energy efficient protocol for WSNs, was presented. ECHERP considers the current and the estimated future residual energy of the nodes, along with the number of rounds that can be cluster heads in order to maximize the network lifetime. In future work, ECHERP can be further enhanced by taking into consideration metrics related to QoS and time constraints. We have presented a new key predistribution scheme that uses region-based deployment knowledge to assign keys to sensor nodes. Our simulation results show a significant improvement in resilience over existing schemes using region-based deployment knowledge. Future work can be done to characterize the effects of localized network attacks, as well as the effects of different deployment distributions.

REFERENCES

[1] J.M. Kahn, R.H. Katz, and K.S.J. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," Proc. Ann. ACM/IEEE MobiCom, pp. 483-492, 1999.

[2] G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, no. 5, pp. 551-558, 2000.

[3] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 41-47, Nov. 2002.

[4] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp Security and Privacy, pp. 197-213, May 2003.

[5] A.K. Das, "An Identity-Based Random Key Pre-Distribution Scheme for Direct Key Establishment to Prevent Attacks in Wireless Sensor Networks," Int'l J. Network Security, vol. 6, no. 2, pp. 134-144, 2008

[6] J. Lee and D.R. Stinson, "Deterministic Key Predistribution Schemes for Distributed Sensor Networks," Proc. Ann. Symp. Selected Areas in Cryptography, pp. 294-307, 2004

[7] S.A. C¸ amtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," Proc. Ninth European Symp. Research Computer Security (ESORICS), pp. 293-308, 2004

[8] J. Lee and D.R. Stinson, "A Combinatorial Approach to Key Predistribution for Distributed Sensor Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2005. CD-ROM, paper PHY53-06.

[9] W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," ACM Trans. Information and System Security (TISSEC), vol. 8, no. 2, pp. 228-258, May 2005.

[10] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002.

[11] S. Tilak, N.B. Abu-Ghazaleh, and W. Heinzelman, "A Taxonomy of Wireless Microsensor Network Models," ACM Mobile Computing and Comm. Rev., vol. 6, no. 2, pp. 1-8, 2002

[12] H. Yang et al., "Security in Mobile Ad-Hoc Wireless Networks: Challenges and Solutions," IEEE Wireless Comm. Magazine, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[13] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Networks, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[14] D. Carman, P. Kruus, and B. Matt, "Constraints and Approaches for Distributed Sensor Networks Security," Technical Report 00- 010, NAI Labs, Sept. 2000.

[15] G. Jolly, M. Kuscu, P. Kokate, and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks," Proc. Eighth IEEE Symp Computers and Comm. (ISCC '03), June 2003.

[16] TinySec, http://www.cs.berkeley.edu/nks/tinysec/, 2006.

[17] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computing and Comm. Security (CCS '02), Nov. 2002.

[18] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks" Proc IEEE Symp. Security and Privacy, May 2003.

[19] G. Gupta and M. Younis, "Load-Balanced Clustering in Wireless Sensor Networks," Proc. Int'l Conf. Comm. (ICC '03), May 2003.

[20] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks," IEEE Trans. Mobile Computing, vol. 3, no. 4, pp. 366-379, Oct.-Dec.2004.

[21] K. Langendoen and N. Reijers, "Distributed Localization in Wireless Sensor Networks: A Quantitative Comparison," Computer Networks, vol. 43, no. 4, pp. 499-518, Nov. 2003.

[22] A. Youssef, A. Agrawala, and M. Younis, "Accurate Anchor-Free Localization in Wireless Sensor Networks," Proc First IEEE Workshop Information Assurance in Wireless Sensor Networks (WSNIA '05), Apr. 2005

[23] Lina M. Pestana Leão de Brito and Laura M. Rodríguez Peralta, "An Analysis of Localization Problems and Solutions in Wireless Sensor Networks", Polytechnical Studies Review, 2008, Vol VI, ISSN: 1645-9911.

[24] Huang Lee and Hamid Aghajan, "Collaborative Self-Localization Techniques for Wireless Image Sensor Networks", In Proc. of Asilomar Conf. on Signals, Systems and Computers, Oct. 2005.

[25] D.Saravanan , D.Rajalakshmi and D.Maheswari "DYCRASEN: A Dynamic Cryptographic AsymmetricKey Management for Sensor Network using Hash Function", International Journal of Computer Applications (0975 – 8887) Volume 18– No.8, March 2011

[26] Yoon-Su Jeong, and Sang-Ho Lee "Secure Key Management Protocol in the Wireless Sensor Network", International Journal of Information Processing Systems, Vol.2, No.1, March 2006.

[27] Mohammed A. Abuhelaleh and Khaled M. Elleithy "SECURITY IN WIRELESS SENSOR NETWORKS: KEY MANAGEMENT MODULE IN SOOAWSN", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[28] P. F. Oliveira, R. A. Costa, and J. Barros, "Mobile secret key distribution with network coding," presented at the Int. Conf. Security Cryptography, Jul. 2007.

[29] P. F. Oliveira and J. Barros, "Network coding protocols for secret key distribution," in Proc. Int Symp Information Security, Nov. 2007, pp. 1718–1733

[30] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.

[31] D. Malan, M. Welsh, and M. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," presented at the 1st IEEE Int. Conf. Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, Oct. 2004. [Online]. Available: citeseer. ist.psu.edu/malan 04publickey.html.