I.J. Computer Network and Information Security, **2014, 4, 29-36**
Published Online March 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.04.04

A Comparative Study of Key Management Protocols for WSN

Seema Verma
Department of Electronics Banasthali University, Rajasthan, India
Email: seemaverma3@yahoo.com

Prachi
CSE & IT Department ITM University, Gurgaon, India
Email: prachiah1985@gmail.com

Abstract — Increased employment of WSN (Wireless Sensor Network) in real life applications and their hostile and remote locations accelerate demand of security in WSN. Publicly accessible wireless communication channel also makes WSN vulnerable to numerous security attacks. Scarcity of resources acquaints new sort of challenges and difficulties during implementation of effective security mechanisms. In this paper, we evaluate and compare performance of three different security mechanisms (ECRKS, CKP and AP scheme). ECRKS (Energy-efficient, Connected, Resilient Key pre-distribution Scheme) is based upon multi hop communication architecture specifically designed for homogeneous WSN. Clustering based protocols, AP (Asymmetric pre-distribution) scheme and CKP (Clustering based Key management Protocol) are proposed for heterogeneous WSN. All the above mentioned schemes are simulated in MATLAB to evaluate their effectiveness and suitability for WSN. Simulation result shows that CKP outperforms other two schemes in terms of transmission distance, memory burden, energy dissipation and resilience.

Index Terms — Energy; key; memory; security; WSN.

I. INTRODUCTION

Research in WSN has flourished because researchers are contemplating WSN deployment in various challenging circumstances (such as logistics, automation and control) where deployment of wired networks is impractical. WSN is usually implanted in a harsh/hostile environment without human intervention so adversary can easily snoops information from sensors deployed in remote locations. Before incorporating WSN in real life applications for continuous monitoring it is important to prove their trustworthiness and make them robust against various security threats. Applications that involve life-threatening scenarios such as nuclear reactors, e-healthcare and military application decision is based on information gathered by sensors so usage of WSN in various information sensitive applications is only feasible and practical if we can actually trust their readings and strategic decisions are based on correctly retrieved information and not derived from malicious information. Unreliable and high-bit error rate wireless communication channel accelerates the requirement of secure transmission because publicly accessible channel is vulnerable to numerous security attacks. An adversary can easily intercept the information transmitted through the publicly accessible channel to tamper information or to inject false messages in the network. Moreover, the adversary can compromise any node to retrieve all information stored in its memory because sensors are usually deployed in vicinity of the physical environment of event detection and it is impractical to assume that sensors are tamper proof due to cost constraint. So, the security of information is extremely crucial to prevent attacks from influencing the functionality of network and securing WSN in an effective and efficient manner is very imperative because unlike traditional network security is an auxiliary operation for WSN. To secure information, cryptography became essential. Cryptosystems can be categorized as asymmetric cryptosystem and symmetric cryptosystem. Asymmetric cryptosystem (self enforcing schemes) offers a high level of security using public key cryptography for the generation and distribution of keys. These schemes are perfectly resilient as they will not reveal anything about other keys of network so most suitable for WSN because they are generally deployed in hostile and unattended environments. Public key cryptosystems offer high resilience. However, their demand for huge storage and computational power make them infeasible for sensor networks.

Symmetric encryption algorithms are lightweight in terms of resources when compared to asymmetric algorithms so most suitable for WSN. In this paper, we evaluate three security protocols (ECRKS, CKP and AP scheme) to determine which one suits best to the requirements of WSN. ECKRS is developed for homogeneous WSN and AP scheme and CKP are developed for heterogeneous WSN.

Remainder of this paper is organized as follows.

Manuscript received November 12, 2013; accepted December 16, 2013.

Related work is discussed in section II. Section III provides description of ECRKS, CKP and AP scheme. Simulation and performance evaluation is performed in section IV. Finally, section V draws conclusion.

II. RELATED WORKS

Key management protocols are linchpin to implement any kind of cryptographic suite. Considering security importance in WSN, several key management protocols were proposed in literature to address their security requirements. Most of the protocols were designed for homogeneous network. First of all, we discuss some of the symmetric security schemes proposed in literature for homogeneous networks (where all sensors have similar capabilities in terms of battery, processor and transceiver). Single shared key schemes [1-3] are simplest schemes where all nodes of the network share a secret key. These types of schemes are efficient, flexible and require minimum storage overhead irrespective of size of the network. Moreover, any number of nodes can be added in the network simply by loading them with a single key. Single shared key schemes offer maximum level of connectivity. Although single shared key schemes offer numerous advantages but they not resilient because a single compromised node reveals entire communication of the network. Moreover, the attacker can easily insert any number of malicious nodes simply by loading nodes with master key. Another variation is full pairwise key schemes [4-5] where every node stores n-1 keys for the network of size n to communicate with every other node of network. These types of schemes provide prefect resilience and node-to-node authentication. However, full pairwise schemes induce very huge memory burden on resource constrained nodes. Additionally, full pairwise key schemes limit scalability as addition of any new node requires change in all existing nodes of the network. A group based key management schemes [6-7] are lightweight but cannot offer a high amount of security. Trusted third party became a bottleneck and single point of failure in trusted third party based key management schemes [8-9]. Also, these schemes are very time consuming. Matrix based key distribution [10-11] and polynomial based key distribution schemes [12] suffer from large storage and computation burden. Hash based key distribution schemes [13-14] improve security but again computation processing is high due to hash function computations. Computation further increases energy consumption of nodes. Location based key distribution schemes [15-16] assumes prior knowledge about the topology of network. Availability of prior location information is quite impossible in WSN due to random deployment and frequent topology changes.

A number of probabilistic approaches [17-23] were presented in literature. Probabilistic key pre-distribution schemes reduce storage and communication burden up to a certain extent so they are considered as a most efficient scheme for homogeneous WSN. In these types of schemes, nodes are preloaded with a small number of keys such that every node shares keys with other nodes with certain probability such that network always remains connected. Probabilistic key management protocols were first introduced by Eschenauer et al. in [17] to reduce storage requirement where each node is preloaded with k keys randomly selected from large size pool (P) where (k<<P). If nodes in transmission range share keys together then nodes can communication by encrypting communication with shared key. If two nodes don't share a key then they establish an indirect path through intermediate nodes to which both nodes are directly linked. This scheme exclude overhead of implementing BS. Main problem with this scheme is that it reveals communication between non-compromised nodes when other nodes are compromised due to sharing of keys among compromised and non-compromised nodes. This scheme is popular as EG scheme (basic scheme). To make EG scheme further resilient Chan et al. proposed q-composite scheme based on EG scheme [18]. Two nodes can only communicate if they share at least q keys in common where q>=1. Q-composite scheme is more resilient than EG scheme when number of compromised nodes is less than a threshold because adversary needs to capture more keys to compromise communication among the nodes. To increase number of shared keys among nodes, P should be small. With small P, capturing a few nodes reveal entire pool. If we increase P, scheme became resilient but probability of sharing keys among nodes decreases. EG and q-composite reduce storage burden upto some extent but suffer from huge communication overhead. Session key scheme [19] was introduced by Hussain et al. where session key is computed by initially shared key among the nodes, hash function, publicly known seed and an array. This scheme boosts little security compared to communication and computation burden it increases. Dynamic key generation using one-way hash function was proposed by Kesawan et al. in [20]. This scheme provides high security due to storage of keys in non-volatile memory. This scheme involves huge communication burden due to time synchronization among nodes and high storage requirement at nodes because of dynamic generation of keys. It is clear from the above discussion that all the above mentioned security scheme involve huge communication burden. Security protocol should have minimum communication requirement because sensors comes with extra limited resources and energy consumption involved in communication is about 98% of overall energy consumption.

To reduce the communication burden and redundancy of information, clustering was proposed as a solution. Clustering can be implemented in two forms: static and dynamic. Static clustering is suggested as an energy-efficient, scalable and high performance communication model. In static clustering, cluster and CH are fixed throughout the entire lifetime of network. CH performs various tasks such as data aggregation, transmission, reception and listening that lead to fast depletion of energy when compared to rest of the sensors. Static

clustering suffers from a hotspot problem in homogeneous network. To remove hotspot problem, dynamic clustering communication architecture was pioneered by Heinzelman et al. in [24] known as LEACH (Low Energy Adaptive Clustering Hierarchy) and a number of variations [25-26] were proposed afterwards. In LEACH, all nodes exhibit same hardware complexities (high range modem, aggregator etc). LEACH removes the hot spot problem by rotating CH to evenly distribute energy dissipation over all nodes of network. LEACH doesn't assure optimal coverage of network due to random election of CH based on residual energy of nodes. Nodes broadcast their residual energy at fixed intervals and based on their residual energy, some of the nodes are chosen as CH. Repeated election of CH and reorganization of cluster are very energy intensive operations that drain maximum amount of energy from dynamic clustering protocols.

A number of security schemes have been presented in literature but majority of them are designed for homogeneous networks. However, it has been advocated in recent research [27-30] that heterogeneous WSNs offer much better performance and lifetime than homogeneous WSN with very less additional cost. In heterogeneous network, some high power nodes are implemented with a large number of low power nodes. According to [27], homogeneous network only try to minimize energy consumption but heterogeneous network reduce overall cost by embedding hardware complexity (high power battery, high transmission range modem, aggregator etc) in few nodes rather than implementing it in all nodes of network. Authors in [29] suggest that heterogeneous nodes increase reliability, network lifetime and discuss computational, energy and link heterogeneity. Result depicts that by embedding less than 10% of heterogeneous nodes network lifetime increases more than five times. Static clustering can work well with heterogeneous WSN where high power nodes are assigned majority of task. Authors in [31] used the idea of static clustering and presented a clustering based key pre-distribution scheme (AP scheme) for heterogeneous WSN. Other security schemes [32-33] were also presented for heterogeneous WSN. One of them demonstrates power of unbalanced key distribution for different trust models and other created a secure tree rooted at sink to minimize storage at low power sensor nodes.

III. DECRIPTION OF SECURITY PROTOCOLS

This scheme provides theoretical description about ECRKS, CKP and AP scheme.

A. ECRKS

ECRKS scheme [34] is built upon the EG scheme while proposing improvements. ECRKS increases probability of connectivity, resilience, fault tolerance and reduces communication overhead, power depletion and memory overhead significantly over EG scheme under variable network sizes and traffic loads. ECRKS comprises of three different phases: Key Generation and Pre-Distribution phase, Single hop key establishment phase and Multi hop key establishment phase. During key generation and pre-distribution phase, a key pool of a large number of keys is generated using a pseudo random number generator along-with their identifiers (ids). Each node is randomly assigned certain number of keys from key pool and require to establish key with d nearest possible neighbors where d is degree of node in network.

During single hop key establishment phase, nodes broadcast their list of key ids, node ids and location information. Two nearest possible nodes (A and B) that are within communication range and share same key id establish secure communication with the help of shared key. If a node doesn't share a key or not in communication range with d nodes then A stores key ids of nearest neighbor, say B and goes to multi hop key establishment phase. During multi-hop key establishment phase, node A selects an intermediate node (C) from its neighbors such that C shares keys with A and B and average distance of node C from A and B remains minimized. Energy consumption is directly proportional to the square of distance so nearest intermediate node is chosen in order to reduce energy consumption of nodes. During multi hop key establishment phase, ECRKS reduces transmission distance of more than 78% links. Additionally, EG scheme involves broadcast of key ids of A and B ids during multi hop key establishment phase. Broadcasting is extremely challenging in WSN because it consumes lots of bandwidth and energy. Moreover, double size of message further increase energy dissipation. Unlike EG scheme, ECRKS removes broadcast from multi-hop key establishment phase to efficiently utilize resources.

To further enhance security, whenever A and B don't share a key new key is not chosen from key ring of C but C randomly selects a key from key pool and send to A and B in a secured manner. In this way, even if C is captured by adversary communication between A and B is not compromised. We implemented ECRKS on random graph theory proposed by Erdos-Renyi (ER) model [35] because this model is adopted by majority of key pre-distribution protocols. However, the authors in [36] suggested that ER model is not suitable for WSN due to its unrealistic assumptions of unlimited transmission range and insertion of new edge irrespective of connectivity provided by previously inserted edges. So, we also implemented ECRKS on random graph theory proposed by cryptograph model [36] that offer both restricted transmission range and insertion of any edge is dependent on the connectivity offered by already existing edges.

B. AP Scheme

AP scheme was presented for heterogeneous WSN based on the concept of static clustering and ER model. Here, H-sensors (High-end sensors) and L-sensors (Low-end sensors) are randomly distributed over the geographical region of network. H-sensors are

designated as CHs. Each cluster is governed by a CH. During initialization of network, H-sensors broadcast a HELLO message in network with random delay to avoid collisions with nearby CHs. Choice of nearest CH leads to cluster formation phase. L-sensors choose their nearest CH and save details about other CHs so that they can serve as backup CH if nearest CH fails. The AP scheme comprises of three phases: key pre-distribution phase, shared-key discovery phase and H-sensor based pairwise key setup phase. During key pre-distribution phase, a large size pool of keys and their ids is generated. Each L-sensor is assigned to l keys randomly selected from key pool without replacement. Each H-sensor is also assigned M (M>>l) keys randomly selected from key pool without replacement. Additionally, CH is assigned with a key kH known to BS not to L-sensors. Shared key discovery phase can be performed in a centralized or distributed manner. In distributed manner, each L-sensor broadcasts its list of key ids to neighbor nodes to determine whether it shares any key with neighbors or not. In centralized way, the L-sensor broadcasts its list of key ids, node id and location information to CH. Now, CH determines nodes that share common key and also fall within transmission range. After determining a shared key, CH sends a triplet that contains sender's id, destination's id and shared key among them. During pair-wise key setup phase, if a pair (x and y) in a cluster don't share a key together then CH finds a shared key with x and a shared key with y and generates a new key for them. Now, CH sends this new key to x and y securely by encrypting it with keys shared with x and y. There is a high probability that CH will find a shared key with both of them because CH is preloaded with large number of keys. A L-sensor that shares at least one key with H-sensor is known as its 1st degree neighbor. If CH doesn't share a key with any of the sensors then CH will find its 1st degree neighbor that shares keys with its sensors. If CH finds z as its 1st degree neighbor that shares key with its sensor then CH sends a newly generated key to its sensor through z by encrypting it with key shared with z. If none of CH 1st degree neighbors share a key with its sensor then CH will look for 2nd degree neighbors and so on until it finds a node that shares a key with its sensor. If none of its neighbors have a shared key with its sensor then CH will send a request to BS including one of the key ids of its sensor and BS sends corresponding key by encrypting it with kH.

C. CKP

CKP [37] is a static clustering based protocol designed for heterogeneous WSN. Prior to deployment in field, each L-sensor is loaded with a unique key and id. Unique key is used to encrypt communication between sensors and CH. CHs are placed at pre-determined location of network in order to provide optimal coverage and each CH shares a unique key with BS (Base Station). BS is a very high power system that interacts with end users via wireless or wired communication channel. BS offers intrusion detection system to find malicious behavior of nodes. Surface station (SS) is another authentic device that generates ids of nodes and maintains a database regarding keys of all members of network. It is also used by CHs for authentication of their members. CHs periodically broadcast join request messages to network with high transmission power. Message comprises of CH id and timestamp. The timestamp is used to avoid replay attack and ensure freshness of message. After receiving messages from multiple CHs, L-sensors choose their nearest CH and send join response message to it. Nearest CH is chosen in order to minimize power dissipation of L-sensors during transmission of signal. Before allowing L-sensors to join cluster, every CH authenticates sensors from whom it gets to join response message. For authentication, CH forwards list of L-sensors ids to SS. SS authenticates L-sensors ids using its database. CH also calculates MAC and incorporates it into message along-with list of L-sensors ids so that we can easily identify changes if an eavesdropper tries to modify list of L-sensors ids. After receiving messages from CH, BS checks list for unauthentic node id and deletes them from the list, if found any. BS forwards list of authentic L-sensor ids along-with their preloaded keys to CH by encrypting messages with key uniquely shared between CH and BS. After receiving list from BS, CH decrypts the message and recalculates MAC. If MAC matches, CH retrieves L-sensors ids and their keys. Now, CH acknowledges L-sensors to join the cluster. An acknowledgement message comprises of several sub messages where each sub message is encrypted with the pair-wise wise key (sent by BS to CH respective to each member) shared between L-sensor and CH. This key is used to secure communication between L-sensor and CH.

IV. SIMULATION AND PERFORMANCE EVALUATION

This section simulates ECRKS, AP and CKP security schemes in order to evaluate effectiveness and performance of these schemes under variable size networks.

A. Simulation Environment

Numbers of scenarios are executed with variable number of nodes ranging from 40 to 160 in steps of 40 deployed in region of 2800*2800m2. Transmission technology is radio. Table 1 shows simulation parameters in detail.

TABLE 1: Simulation parameters & their values

Parameter	Value
Security protocols	ECRKS, AP, CKP
Placement model	Random
Transmission range	1500m
Traffic type	Constant bit rate
Antenna model	Omni directional
Area	2800m*2800m
Node id	32 bit
Key size	128 bit
MAC	160 bit
Timestamp	128 bit
Location information	64 bit

B. Performance index

- Distance refers to average transmission distance of a message from source node to BS delivered over the network via radio links.
- Energy refers to total energy dissipation in transmission of a message from source node to BS delivered over the network via radio links.
- Memory refers to total storage requirement of a sensor node to store data required by corresponding storage scheme.
- Location of CH effects coverage of network and transmission distance of nodes within that cluster.
- Resilience refers to probability of finding a key of non-compromised node from the set of key rings of compromised nodes.

C. Performance Evaluation

We simulate different network scenarios to evaluate effect of varying number of nodes on transmission distance, memory overhead and energy consumption for all three schemes. Further, we evaluate effect of location of CH on transmission distance and probability of compromisation vs number of compromised nodes.

C.1 Distance vs Number of nodes

Fig. 1 demonstrates the transmission distance of nodes in meters with respect to number of nodes in network. It is clear from the picture that the transmission distance of packets in clusters based security schemes (CKP and AP scheme) is much shorter than transmission distance of packets in any multi-hop based security scheme. Further, note that CKP outperforms AP scheme in terms of transmission distance (i.e. packets in CKP travel minimum distance) because CH are placed at pre-determined locations to minimize the distance instead of randomly distributing throughout the network. Shorter propagation distance leads to small transmission time and less transmission power.

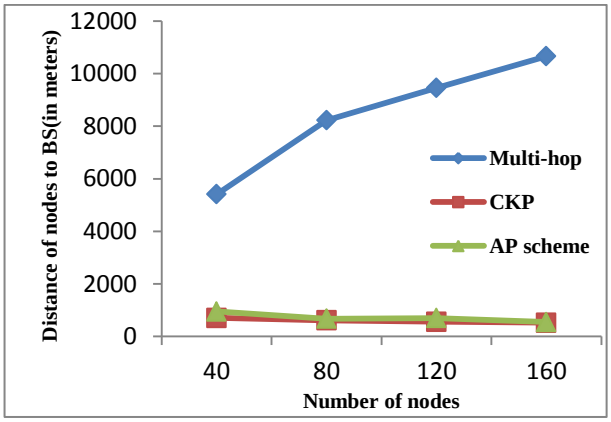

Figure 1. Transmission distance vs Number of nodes

C.2 Memory vs Number of nodes

Fig. 2 shows total memory requirement of network with respect to number of nodes. Simulation results show that memory requirement of AP scheme increases very rapidly as size of network grows. CKP and ECRKS have similar memory overhead and it doesn't increase much with network size. Memory burden on L-sensors of CKP are even less than memory required by sensors in ECRKS.

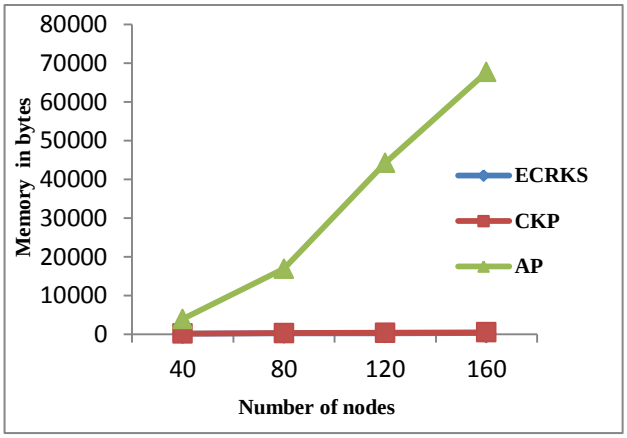

Figure 2. Memory vs Number of nodes

C.3 Energy consumption vs Number of nodes

As shown in fig. 3, energy consumption is highest in AP scheme due to transmission of large size packets comprising of enormous number of keys. Moreover, radio energy consumption model proposed in [38] states that energy consumption is directly proportional to square of distance and number of bits. Huge memory burden of AP scheme leads to high energy dissipation. ECRKS also consumes high energy due large transmission distance as shown in fig. 1. CKP performs best by consuming least amount of energy due to small transmission distances and packet size.

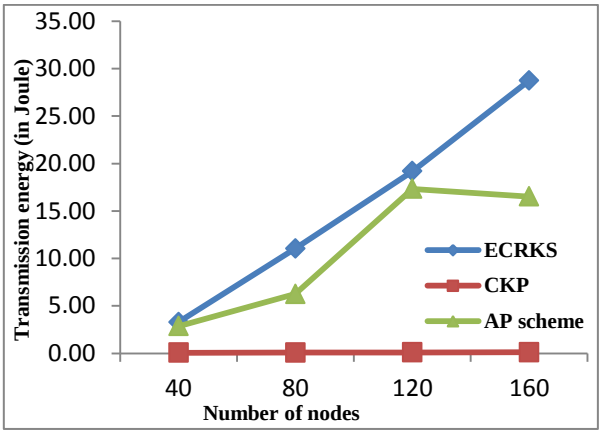

Figure 3. Energy Consumption vs Number of nodes

C.4 Location of CH

In CKP and AP scheme, location of CHs is significant in order to provide optimal coverage of network and minimize transmission distance of nodes from its CH. Randomly placed CHs in AP scheme cannot achieve optimal coverage of network because sometimes two or more CHs exist in neighboring. In CKP, CHs are placed at pre-determined locations of network to provide optimal coverage. Pre-determined locations of CHs not only provide optimal coverage but also reduce distance of nodes from their CHs. As discussed earlier, reduction in transmission distance of signal decreases energy consumption and also retains quality of signal.

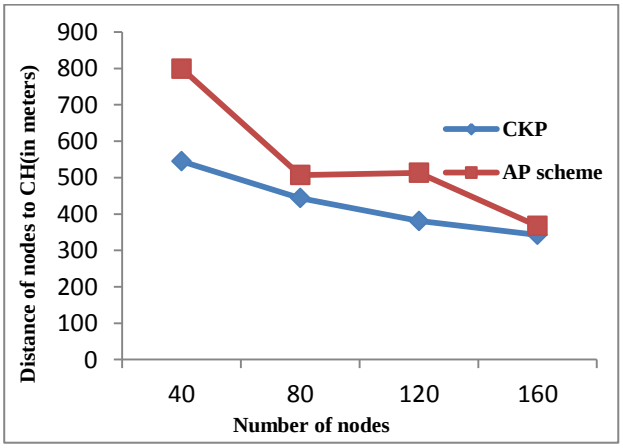

Figure 4. Distance of nodes from CH vs Number of nodes

Fig. 4 depicts average transmission distance of nodes from their CH with respect to number of nodes. Results demonstrate that distance of nodes in CKP scheme is lower than distance of nodes in AP scheme. So, CKP reduces transmission distance which in turn reduces energy dissipation and retains quality of signal at receiver's side.

C.5 Resilience

ECRKS and AP scheme have similar probabilities of compromisation for different number of compromised nodes because H-sensors in AP scheme are assumed to be tamper resistant. Probability of determining key k of non-compromised node in ER model is given as:

$$1-\left(1-\frac{l}{P}\right)^{c} \tag{1}$$

where, l is number of keys possessed by a sensor (L-sensor in AP scheme), P is the size of key pool and c is number of compromised nodes. In cryptograph model, high resilience is assured if (2) satisfies:

$$\frac{l}{P} \sim \frac{1}{n} \tag{2}$$

where n is number of nodes in network

Results shown in fig. 5 illustrate that resilience of ECRKS increases significantly when implemented in cryptograph model.

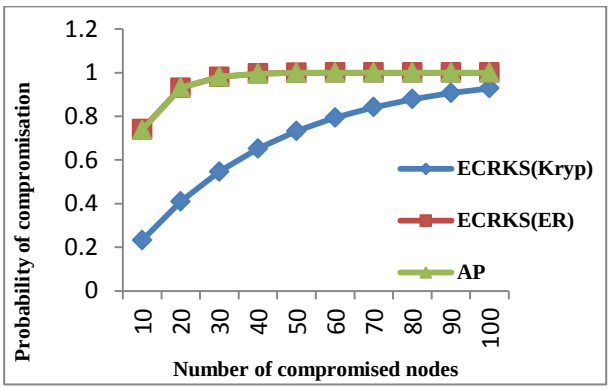

Figure 5: Probability of compromisation vs Number of compromised nodes

In CKP, each L-sensor stores a single key shared with CH so if a node is captured by adversary then captured node reveals only one key associated with that node and it will not affect security of any other node. So, CKP offers optimal resilience whereas in other two protocols it is possible to retrieve some of the keys of non-compromised nodes from captured nodes because there is a high probability of sharing keys between nodes due to their random selection from the pool.

VI. CONCLUSIONS

Security of sensitive information is exceptionally important in WSNs due to their rapid usage in real life applications and resource exhaustion attacks because of sensor's resource stringent nature. In this paper, we have compared three security protocols based on energy dissipation, memory burden, transmission distance and resilience. Simulation results conclude that CKP and ECRKS perform better than AP scheme in terms of memory burden and energy consumption. ECRKS suffers from high transmission distances (leads to high

propagation time and poor quality of received signal) and security issues. AP scheme induces high memory burden due to a large number of keys and high energy dissipation because of huge size messages. CKP performs better on all parameters than other two security schemes and proves its suitability for WSN.

REFERENCES

[1] B. Lai, S. Kim and I. Verbauwhede. Scalable Session Key Construction Protocols for Wireless Sensor Networks. In Proceedings of the IEEE Workshop on Large Scale RealTime and Embedded Systems, pp. 1-6, 2002.

[2] ZigBee Alliance. Zigbee specification document 053474r06, v1.0.Technical report, ZigBee Alliance, 2004.

[3] Y. Zeng, B. Zhao, J. Su, X. Yan and Z. Shao. A loop-based key management scheme for wireless sensor networks. Workshop on Emerging Directions in Embedded and Ubiquitous Computing, 2007. 4809: p. 103–114.

[4] H. Chan and A. Perrig. PIKE: peer intermediaries for key establishment in sensor networks. In proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005. 1: p. 524–535.

[5] H. Chan, V. Gligor, A. Perrig and G. Muralidharan. On the distribution and revocation of cryptographic keys in sensor networks. IEEE Transactions on Dependable and Secure Computing, 2005. 2(3): p. 233–247.

[6] J. M. Kim and T. H. Cho. A*-based key tree structure generation for group key management in wireless sensor networks. Computer Communications, 2008. 31: p. 2414–2419.

[7] F. Wu, H. T. Pai, X. Zhu, P. Y. Hsueh and Y. H. Hu. An adaptable and scalable group access control scheme for managing wireless sensor networks. Telematics and Informatics, 2013. 30: p. 144–157.

[8] J. Kohl and B. C. Neuman, The Kerberos Network Authentication Service (Version 5). Internet Request for Comments RFC-1510, 1993.

[9] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. Wireless Networks, 2002. 8: p. 521-534.

[10] 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 Transactions on Information and System Security, 2005. 8(2): p. 228-258.

[11] M. Rahman, S. Sampalli and S. Hussain. A Robust Pair-wise and Group Key Management Protocol for Wireless Sensor Network. In 2010 IEEE GLOBECOM Workshops, 2010, pp. 1528-1532.

[12] D. Liu and P. Ning. Establishing Pairwise Keys in Distributed Sensor Networks. In proceedings of the 10th ACM conference on Computer and communications security. pp. 52-61, 2003.

[13] W. Bechkit, Y. Challal and A. Bouabdallah. A new class of Hash-Chain based key pre-distribution schemes for WSN. Computer Communications, 2013. 36(3): p. 243–255.

[14] W. Bechkit, Y. Challal and A. Bouabdallah. An Efficient and Highly Resilient Key Management Scheme for Wireless Sensor Networks. In 35th Annual IEEE Conference on Local Computer Networks, pp. 216 – 219, 2010.

[15] K. Ren, W. Lou and Y. Zhang. LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. IEEE Transactions On Mobile Computing, 2008. 7(5), p. 585-598.

[16] A. Gaur, S. Toshniwal, A. Prakash and D. P. Agrawal. Enhanced Location Based Key Pre-Distribution Scheme for Secure Communication in Wireless Sensor Network (WSN). In 2010 IEEE 7th International Conference on Mobile Adhoc and Sensor Systems, pp. 552-557, 2010.

[17] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of 9th ACM conference Computer and Communication Security, pp. 41-47, 2002.

[18] H. Chan, A. Perrig and D. Song. Random key predistribution schemes for sensor networks. In Proceedings of 2003 IEEE Symposium on Security and Privacy, pp. 197-213, 2003.

[19] Hussain, S., Rahman, M., Yang, L. Key predistribution scheme using keyed-hash chain and multipath key reinforcement for wireless sensor networks. IEEE Computer Society, Los Alamitos, CA, USA, 2009, pp. 1–6. doi:10.1109/PERCOM.2009.4912893.

[20] Kesavan, V. T., Radhakrishnan, S. Multiple Secret Keys based Security for Wireless Sensor Networks. In International Journal of Communication Networks and Information Security (IJCNIS), 2012. 4(1): p. 68-76.

[21] W. Bechkit, Y. Challal, A. Bouabdallah and V. Tarokh. A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. IEEE Transactions on Wireless Communications, 2013. 12(2): pp. 948-959.

[22] C. Castelluccia and A. Spognardi. RoK: A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks. In Proceedings of 3rd International ICST Conference on Security and Privacy in Communication Networks, pp. 351-360, 2007.

[23] S. Lawrence, L. Qiaoliang, N. Mary and F. Bo. Key Pre-Distribution and the Average Distance in Wireless Sensor Networks. In Second International Conference on Computer and Network Technology, pp. 212–216, 2010.

[24] W. Heinzelman, A. Chandrakasan and H. Balakrishnan. Energy-efficient communication protocol for wireless micro sensor networks. In Proceedings of 33rd Annual Hawaii International Conference on System Sciences, pp. 3005-3014, 2000.

[25] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, An application-specific protocol architecture for wireless micro sensor networks, IEEE Transactions on Wireless Communications, 2002. 1: p. 660-670.
[26] O. Younis and S. Fahmy. Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on Mobile Computing, 2004. 3: p. 366-379.
[27] L. Girod, T. Stathopoulos, N. Ramanathan, J. Elson, D. Estrin, E. Osterweil and T. Schoellhammer, T, "A system for simulation, emulation, and deployment of heterogeneous sensor networks," In proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 201-213, 2004.
[28] V. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar and N. Shroff. A minimum cost heterogeneous sensor network with a lifetime constraint. IEEE Transactions on Mobile Computing, 2005. 4: p. 4-15.
[29] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu and S. Singh. Exploiting heterogeneity in sensor networks. In proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005. 2: p. 878-890.
[30] X. Du and Y. Xiao. Energy efficient chessboard clustering and routing in heterogeneous sensor network. International Journal of Wireless and Mobile Computing, 2006. 1: p. 121-130.
[31] X. Du, Y. Xiao, M. Guizani, and H. Chen. An effective key management scheme for heterogeneous sensor networks. Ad Hoc Networks, 2007. 5: p. 24-34.
[32] P. Traynor, H. Choi, G. Cao, S. Zhu and T. L. Porta. Establishing Pair-wise Keys in Heterogeneous Sensor Networks. In proceedings of 25th IEEE International Conference on Computer Communications, pp. 1-12, 2006.
[33] B. Maala, Y. Challal and A. Bouabdallah. HERO: Hierarchical Key Management Protocol for Heterogeneous Wireless Sensor Networks. In proceeding of Wireless Sensor and Actor Networks II IFIP – The International Federation for Information Processing, 2008. 264: p. 125-136.
[34] S. Verma and Prachi. Key Pre-distribution Scheme for WSNs. Ad Hoc & Sensor Wireless Networks (Accepted).
[35] J. Spencer. The Strange Logic of Random Graphs. Algorithms and Combinatorics, vol. 22. Springer-Verlag, 2000.
[36] R. D. Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Redoubtable Sensor Networks. ACM Transactions on Information and Systems Security, 2008. 11(3): pp.13.1-13.22.
[37] S. Verma and Prachi, "A cluster based key management scheme for underwater wireless sensor network," Communicated.
[38] S. Hussain and A. W. M. Jodrey. Energy efficient hierarchical cluster-based routing for wireless sensor networks. Technical Report - TR-2005-011, 2005.

Seema Verma, Ph. D. and Associate Professor at Department of Electronics in Banasthali University from India.

Her research interests include issues related to communication System, wireless communication, VLSI Design, MIMO - of DM, cryptography & networks security, turbo codes, LDPC codes. She is author of 73 refereed articles in these areas, 30 in reputed international journal and 43 in International Conferences. She has coauthored five books. She is a Fellow of IETE and member of Indian Science Congress, ISTE.

Prachi, Ph. D. student at Banasthali University and Assistant Professor at CSE & IT Department in ITM University from India.

Her research interests include key management protocols in terrestrial wireless sensor networks and underwater wireless sensor networks. She has published 10 research papers in international journals and conference proceedings.

How to cite this paper: Seema Verma, Prachi,"A Comparative Study of Key Management Protocols for WSN", IJCNIS, vol.6, no.4, pp.29-36, 2014. DOI: 10.5815/ijcnis.2014.04.04

