Performance Evaluation of Polynomial Pool-Based Key Pre-Distribution Protocol for Wireless Sensor Network Applications

Malek Ben Amira, Mayssa Bouraoui, Noureddine Boulajfen
Research Center for Microelectronics and Nanotechnology,
Technopole Sousse, 4050
Sousse, Tunisia

***Abstract*—In nowadays, wireless sensor network (WSN) has been established as a leading emerging technology in the field of remote area distributed sensing due to its diverse application areas. Key pre-distribution is an important task in WSN because after the deployment of sensor nodes, their neighbors become strange to each other. To secure the communication, neighbor nodes have to generate a secret shared key, or a key-path must exist between these nodes. In this paper, we have discussed and presented various key pre-distribution protocols, namely, the polynomial pool-based key pre-distribution which is a scheme for creating pairwise keys between sensors on the foundation of a polynomial-based key pre-distribution protocol, introducing two effective instantiations: a *random subset assignment* key pre-distribution scheme and a *grid-based* key pre-distribution scheme. Other studied key pre-distribution schemes (KPDS) are Peer Intermediaries Key for Establishment (PIKE) and Group-based key pre-distribution scheme. The performances of these schemes have been assessed through the simulation of different grids under the TinyOS environment.**

***Keywords*—Key management; wireless sensor network (WSN); key pre-distribution schemes; polynomial pool-based KPDS; PIKE; group-based KPDS**

I. Introduction

Wireless Sensor Network is a group of several resource-constrained sensor nodes that can be accessed via a wireless medium. These sensor nodes are favored because they are low-priced, self-organized and simple to deploy. WSNs are used in military applications, such as military surveillance and battlefield supervision, and civilian ones such as medical monitoring, smart agriculture, etc. [1]. The security of WSNs is a very important aspect which has been actively studied by researchers. Different applications need WSNs to exchange delicate information that necessitate a high level of security to succeed. Yet, strong security is difficult to achieve with limited resources of sensor nodes.

Key management is the element key for security in WSNs because it is the foundation of various security services, like encryption and authentication. The principal goal of key management scheme is to provide secure communication between sensors in the network [2]. But, the critical assignment of key management is the establishment of a pairwise key between two nodes in the network. Different researchers proposed many protocols, such as Polynomial Pool-Based Key Pre-Distribution scheme which has two efficient instantiations: a Random Subset Assignment KPDS and a Grid-based KPDS, Peer Intermediaries Key for Establishment, Group-based KPDS, etc.

In these schemes, the sensors' deployment, which can be randomly or uniformly, can improve the key pre-distribution [3], [4]. So, this paper presents and compares the performances of these different schemes in terms of packet loss rate and energy consumption.

The rest of this article is arranged into six sections. Section 2 presents an overview of the different polynomial-based key pre-distribution techniques and Section 3 introduces the general framework of the polynomial pool-based key pre-distribution and a description of the two instantiations. In Section 4, other key pre-distribution techniques are reviewed. The simulation results are introduced in Section 5. Finally, Section 6 concludes this paper.

II. Polynomial-Based Key Pre-Distribution Schemes

Polynomial-based key pre-distribution protocol [5] is the basis of new techniques such as Polynomial pool-based key pre-distribution. This protocol was created for group key pre-distribution.

The security tolerance of the scheme is decided by the size of security threshold to a great extent [6]. However, once the number of compromised nodes is bigger than the security threshold, the network security performance would be rapidly declined. Besides, to improve the resilience against node capture, the scheme is implemented at the expense of network connectivity [7], [8].

III. Polynomial Pool-Based Key Pre-Distribution

A general framework for key pre-distribution based on the scheme was developed to secure the key establishment techniques. It is called *polynomial pool-based key pre-distribution* [11] due to the use of a pool of many random bivariate polynomials.

The main concept of the polynomial pool-based key pre-distribution can be considered as the combination of the polynomial-based KPDS and the key pool idea consumed in [9] and [10].

Liu and Ning [11] created a general framework for polynomial pool-based pairwise key pre-distribution in wireless sensor networks and two possible instantiations for

key pre-distribution schemes, namely Random Subset Assignment KPDS and Grid-based KPDS [12].

A. Random Subset Assignment KPDS

We introduce in this section, the first possible instantiation of the common framework by employing a random plan for the subset assignment in the set-up phase.

This scheme can be taken as a prolongation to the fundamental probabilistic scheme introduced in [10]. The primary distinctness of this scheme from the basic probabilistic scheme is that it randomly picks polynomials and attributes their polynomial shares to each sensor instead of randomly choosing keys from a big key pool and attributing them to sensors. For that reason, a random subset can be designed as an extension to the fundamental probabilistic scheme [13]. This scheme also differs in the sense that it uses a distinct key for each link [14].

B. Grid-Based KPDS

Another instantiation of the general framework introduced in this section is called grid-based KPDS [15]. This scheme has many interesting properties. First of all, it ensures that even when there are no compromised nodes, any two sensors can create a pairwise key between them and the sensor nodes can report to each other. Second, grid-based KPDS is resilient to node compromise. Even if some sensors are captured, there is still a great chance for the key establishment between the uncompromised nodes using this approach. Third, with grid-based KPDS, a sensor node can define whether or not it can create a pairwise key with another node, and if so, which polynomial should be utilized. As a result, there isn't a communication overhead over the polynomial share discovery.

IV. Other Key Pre-Distibution Techniques

Besides the polynomial pool-based key pre-distribution scheme, various key distribution techniques are implemented, such as Peer Intermediaries Key for Establishment and Group-based key pre-distribution scheme. In this section, we present these schemes so that we can compare them with the Polynomial pool-based KPDS.

A. PIKE

Chan and Perrig [13] proposed a method called Peer Intermediaries Key for Establishment (PIKE) and dedicated to the key establishment. The basic idea behind this scheme is employing peer sensor nodes like trusted intermediaries. PIKE was created to overcome the absence of scalability of the existing symmetric key distribution schemes. Each node shares another (unique) pairwise key with each of the other nodes (O $\sqrt{n}$) in the network.

Each node in Fig. 1 will be loaded with 18 keys (9 keys for the nodes belonging to its line and 9 keys for the nodes belonging to its column). In general, each node stores $2(\sqrt{n}-1)$ keys and the whole number of unique keys generated is $n(\sqrt{n}-1)$.

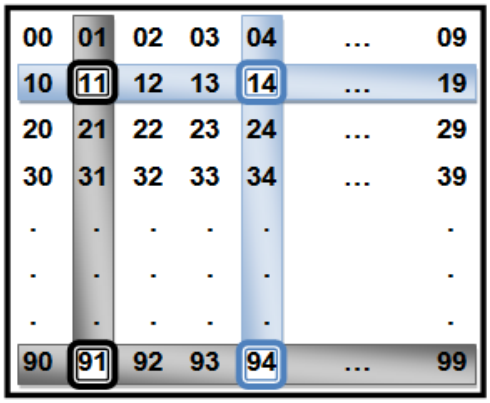

Fig. 1. Virtual space of node identifiers of a network of 100 nodes [16].

B. Group-Based KPDS

In Group-based KPDS, sensors are distributed and organized only in groups [17]. The deployment knowledge utilized to increase the performance of key pre-distribution revolves around the observation that the sensor nodes in the same group are distributed close to each other. This assumption is usually true since the sensor nodes in the same group are assumed to be displayed at the same time from the same point. Once the sensor nodes are displayed in the field, they become static.

Based on this deployment model, the sensor nodes in the same deployment group have an important probability of being neighbors. Group-based KPDS uses two methods, *in-group key pre-distribution* and *cross-group key pre-distribution*.

A sensor node can, without difficulty, assess which displayed group or cross-group other sensor nodes appertain to based on their ID as showed in Fig. 2.

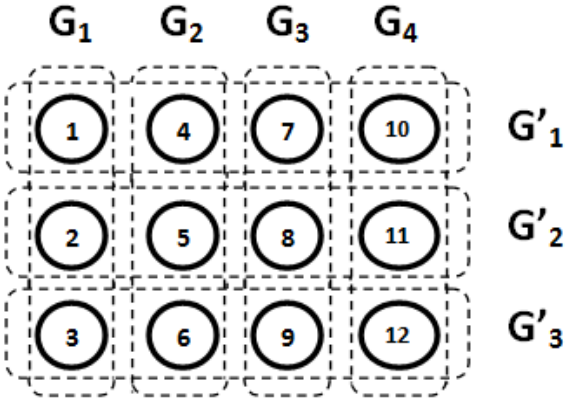

Fig. 2. An example of group construction [17].

V. Simulation and Results

In this section, we assess the performances of Random Subset Assignment KPDS, Grid-based KPDS, PIKE and Group-based KPDS using the TinyOS simulator.

For this purpose, we have simulated random and grid WSNs with 9, 25, 49, 81 and 100 nodes distributed over the field and certain metrics, such as the time of communication between nodes, Packet loss and energy consumption have been measured and compared. The goal behind simulations is to find out the perfect scheme which minimizes the packet loss and energy consumption for each network, and which scheme provides the best probability of establishing a direct and indirect key.

C. Time for Communication between Nodes

Random Subset Assignment KPDS has a random topology which generates a direct communication between two nodes and consequently a direct pairwise key establishment without using an intermediary node. And for Grid-based KPDS, any sensor node can create a direct pairwise key among two nodes.

So in this section, we have studied the time for communication between any two nodes in the network to find which node (sender, intermediary or receiver) and scheme consumes more time in the communication in only PIKE and Group-based KPDS.

Random Subset Assignment KPDS has a random topology which generates a direct communication between two nodes and consequently a direct pairwise key establishment without using an intermediary node. And for Grid-basedKPDS, any sensor node can create a direct pairwise key between two nodes.

So in this section, we have studied the time for communication between any two nodes in the network to find which node (sender, intermediary or receiver) and scheme consumes more time in the communication in only PIKE and Group-based KPDS.

After several simulations of PIKE and Group-based KPDS, it was noted from Fig. 3 that the time to establish a session for the intermediate node is superior to the Sender and Receiver nodes because it needs more time to communicate with them.

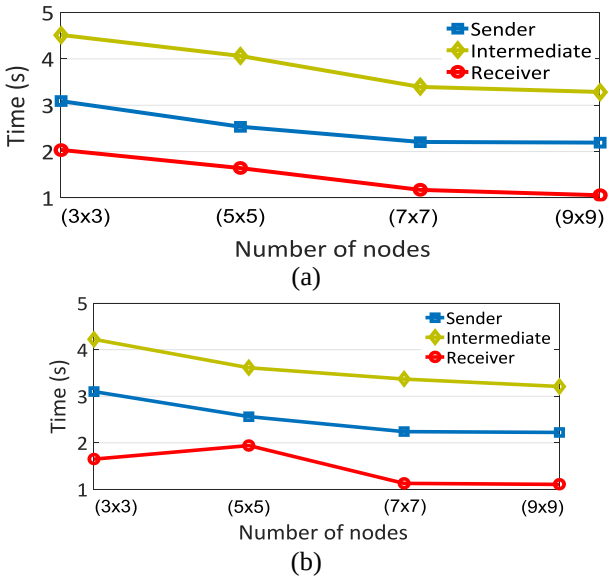

Fig. 3. Time for establishing a session between different nodes for (a) PIKE, (b) Group-based KPDS.

Because once intermediary node is chosen, sender node encrypts the new key to be shared with the receiver node using the key it shares with the intermediary and then sends it to intermediary node. Intermediary node decrypts the key and re-encrypts it using the key it shares with the receiver node, and sends it to receiver node.

After several simulations of the different techniques from 9 to 81 nodes during a fixed-time simulation and in the same area, it was noted from Fig. 4 that the time required for establishing a session is the highest for a network with 9 nodes compared to bigger larger networks because the nodes in each scheme are deployed in the same area, so when the network size increases, the time for establishing a session decreases since the distance between the nodes also decreases.

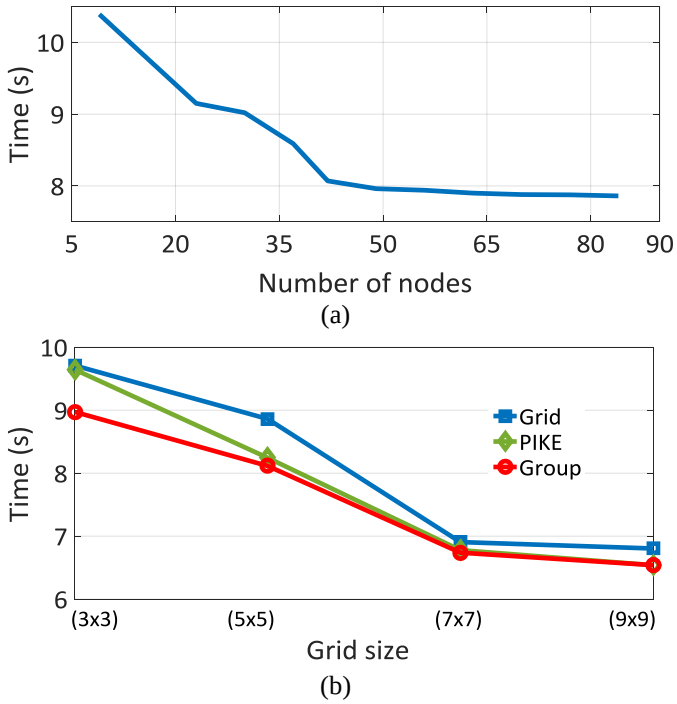

Fig. 4. Time for establishing a session for (a) Random subset assignment KPDS, (b) Grid-based KPDS, PIKE and group-based KPDS.

Among the different schemes, the Random Subset Assignment one consumes more time than others. In this scheme, the sender node requires an intermediate node to send its message to the receiver node, hence going through several intermediate nodes to find the suitable one to share a key with. So, this scheme requires more time than Grid, PIKE and Group-based ones.

D. Packet Loss

We have studied the packet loss caused by the different type of nodes (sender, intermediate and receivers nodes) for the four schemes.

Fig. 5 shows the average packet loss rates for the three groups of nodes for Random Subset Assignment KPDS, Grid-based KPDS, PIKE and Group-based KPDS. We have noticed that the average packet loss reaches the highest level in Random Subset Assignment and the lowest level in Group-based.

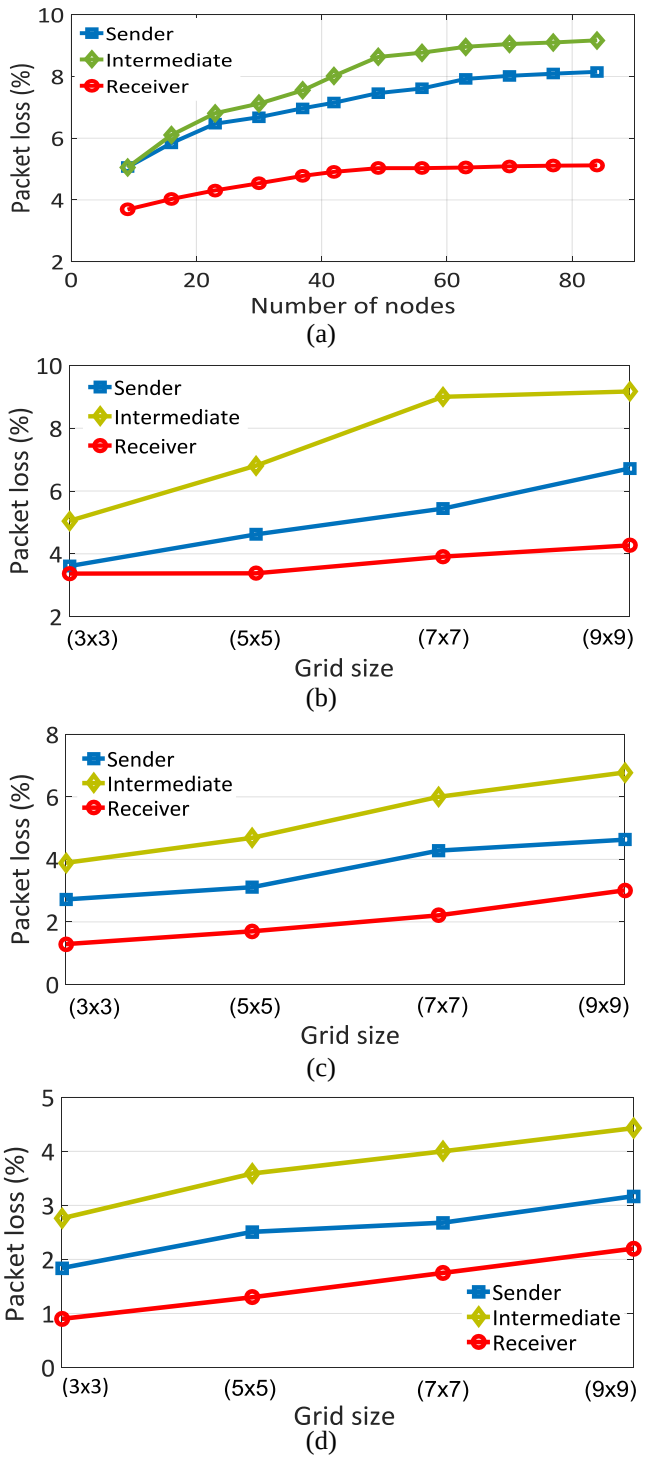

Fig. 5. Average packet loss rate for the "Sender", "Intermediate" and "RECEIVER" NODes for (a) Random subset assignment KPDS, (b) Grid-based KPDS, (c) PIKE and (d) Group-based KPDS.

We have also noticed that when the size of the network increases, the average packet loss rate increases as well.

In Random Subset Assignment KPDS, the overhead storage is low. In addition, sensors can be added without communicating with nodes already deployed in the network. Given some storage constraints and the necessary probability of sharing the direct keys between sensor nodes, the Random Subset Assignment KPDS can allow a limited number of compromised sensor nodes while polynomials pre-distribution scheme can allow a big fraction of compromised nodes. However, due to the affectation of the nodes in a specific order, Grid-based KPDS allows a perfect distribution of nodes so that the sensor nodes can create direct keys which are adjacent to each other. Thus, it can considerably reduce the overhead communication of the key path establishment, which leads to a better packet loss than that of the Random Subset Assignment KPDS. On the other hand, PIKE is a key-establishment protocol that implicates employing one or many sensor nodes as a trusted intermediary to expedite key establishment. Unlike the other protocols, memory overheads and the communication of this protocol help to achieve a higher security against the compromised node and a restricted probability of packet loss compared to other protocols. As for Group-based KPDS, the deployment model is more realistic than the other models, such as Random Subset Assignment KPDS and Grid-based KPDS, because it requires less effort in the deployment of sensor nodes, while providing an opportunity to improve key pre-distribution and a better probability of packet loss.

From Fig. 5 we can note that the intermediate nodes exhibit the highest packet loss rate compared to the sender and receiver nodes for the 4 studied schemes (Random Subset Assignment, Grid-based KPDS, PIKE and Group-based KPDS).

E. Energy Consumption

Fig. 6 reveals that when the size of the network increases, the average energy consumption increases as well. However, the average energy consumption in Random Subset Assignment KPDS is superior to that of the other schemes. For Grid-based KPDS, PIKE and Group-based KPDS, there is no big difference in the average energy consumption, but Group-based KPDS achieves the lowest values.

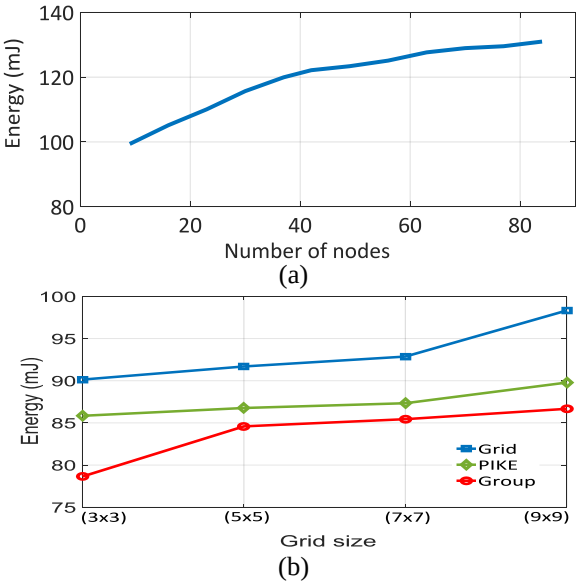

Fig. 6. Average energy consumed by the nodes of the four schemes for (a) Random subset assignment KPDS, (b) Grid-based KPDS, PIKE and group-based KPDS.

Although Grid-based KPDS can guarantee the highest security level, it has certain constraints in terms of the maximum network. Compared to other methods, PIKE minimizes the storage key in the memory nodes before deployment. However, the exchanges of key establishment messages consume time and energy. In PIKE, network nodes are proposed to be used as trusted intermediaries instead of the base station in order to relax nodes close to the base station. However, this solution could be a disadvantage, i.e. if the trusted intermediary nodes *A* and *B* are captured, *A* will no longer share a key with *B*. PIKE has a lower level of memory storage than Random Subset Assignment KPDS, while requiring a communication overhead. This scheme presents many interesting trade-offs in terms of memory and energy overhead compared with the trade-offs available by the other schemes. However, even though the probability of a secure communication between the neighbor "cross-group" is low, Group-based scheme presents a high connectivity and the deployment of sensor nodes is easy and effortless. This scheme presents a strong resilience against attacking nodes, helps to improve key pre-distribution and introduces better energy consumption than the other protocols.

F. Probability of Establishing a Direct and Indirect Key between two Nodes

Fig. 7 shows the results of comparing the four protocols in terms of the direct key establishment. It is noted that when the network size increases, the probability of establishing a direct key between two nodes decreases.

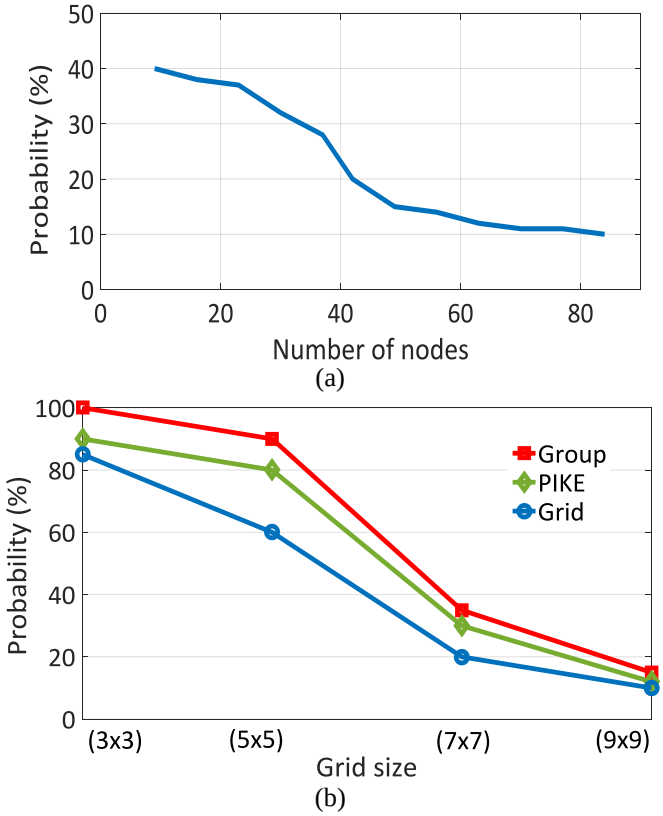

Fig. 7. Probability of establishing a direct key between two nodes for (a) Random subset assignment KPDS, (b) Group-based KPDS, PIKE and grid-based KPDS.

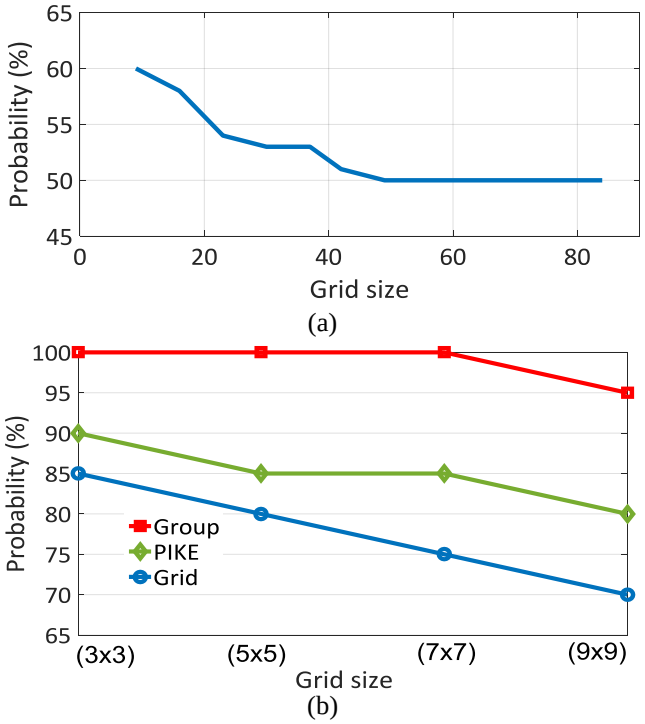

Fig. 8. Probability of establishing an indirect key between two nodes for (a) Random subset assignment KPDS, (b) Grid-based KPDS, PIKE and group-based KPDS.

We can see that Group-based KPDS has certainly a greater probability of establishing a direct key between two sensors than Random Subset Assignment KPDS, PIKE and Grid-based KPDS. This displays that Group-based KPDS can handle an important number of sensor networks with the same network settings.

Although Random Subset Assignment KPDS can be configured to obtain a perfect security, it can support only a restricted number of sensor nodes to guarantee a certain probability of having direct keys between sensor nodes. But, Group-based KPDS can reach a much higher probability to establish direct keys between neighboring nodes than Grid-based KPDS [18]. So, the performance of this scheme is better than that of Grid-based KPDS.

Fig. 8 compares the probability of creating an indirect key between the sensor nodes between the different protocols.

In this part, we consider the probability of an indirect key between two sensor nodes when they cannot create a direct key. We can clearly see from Fig. 8 that the probability of the Group-based KPDS outperforms all other protocols. In other words, as long as the sensor nodes are deployed in groups, Group-based KPDS can be used to obtain high-performance key pre-distribution schemes for sensor networks.

Grid-based KPDS has unique properties which the other schemes do not have. First of all, it is ensured that any two nodes could create a pairwise key either direct or indirect communication and without using an intermediate node when the sensor nodes can be transmitted to each other and in the absence of compromised sensor nodes in the network. In

addition to the efficiency in the determination of the key path, the transmission cost is inferior to that of other systems. In the second place, even if there are compromised nodes in the network, there is an important probability that two non-compromised nodes can restore a pairwise key. For PIKE, this protocol has a uniform communication model for the key establishment, which is difficult to be disturbed by an attacker. Contrary to the current popular mechanisms such as random-key pre-distribution, PIKE has the benefit of a non-probabilistic key establishment, thus whatever two nodes are ensured to establish a key. Also, the probability of having a direct key between two adjacent sensor nodes in the Group-based KPDS is much bigger than that in the Random Subset Assignment KPDS and Grid-based KPDS.

Group-based KPDS has a better security performance than Random subset assignment KPDS at the level of both compromised direct key and compromised indirect key between nodes deployed in the same group of the network.

A comparative study of the various key pre-distribution schemes presented in Table I [19], this comparative study considering the type, scalability, computational overhead, communication overhead, storage load, resilience to node capture and security as the parameters.

TABLE I. COMPARASON BETWEEN THE FOUR SCHEMES

	Random Subset Assignment KPDS	**Grid-Based KPDS**	**PIKE**	**Group-based KPDS**
Type	Prob.	Prob.	Det.	Prob.
Scalability	Good	Good	Not Scalable	Good
Computational overhead	Low	Low	Low	Low
Communication overhead	Low	Low	Low	Low
Storage load	Low	Low	Low	Good
Network Resiliency	Maximal	Maximal	Maximal	Maximal
Nodes Compromised	Yes	Yes	Yes	Yes
Security	Normal	Good	Normal	High

VI. CONCLUSION

In this paper, we presented the polynomial pool-based pairwise key pre-distribution in sensor networks, which is based on the basic polynomial-based key pre-distribution and its two instantiations (key pre distribution scheme based on Random Subset Assignment KPDS and the grid-based KPDS). We have also introduced Peer Intermediaries Key for Establishment and Group-based key pre-distribution scheme.

By simulating these schemes using TinyOS simulator for random and grid networks, we showed that Group-based KPDS is more efficient than the other schemes because it has achieved the lowest values in terms of energy consumption, packet loss rate and time for communication between nodes. Also, Group-based KPDS provides a much higher probability in terms of establishing direct and indirect keys.

Future work introduces the new version of Group-based KPDS, which will be evaluated and compared to PIKE and the standard Group-based KPDS.

REFERENCES

[1] S. Muhammad K. Raazi and S. Lee, “A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks”, Journal of Computing Science and Engineering, Vol. 4, No. 1, Pages 23-51, March 2010.

[2] S. Akhbarfar and A.M. Rahmani, “A Survey on key pre distribution Schemes for security in Wireless Sensor Networks”, International Journal of Computer Networks and Communications Security, Vol. 2, No. 12, 423–442, December 2014.

[3] S. Sibi and A. R Thamizarasi “Key Pre-Distribution Methods of Wireless Sensor Networks” International journal of Scientific & Engineering Research, Vol 4 ,2013.

[4] M. Javanbakht, H. Erfani, H.H. S.Javadi and P.Daneshjoo, “Key Predistribution Scheme for Clustered Hierarchical Wireless Sensor Networks based on Combinatorial Design”, Published online in Wiley Online Library, Vol. 7, No 11, pp 2003–2014, 2014.

[5] C. Blundo, A. Santis, A. Herzberg, S. Kuten, U. Vaccaro and M. Yung, “Perfectly secure key distribution for dynamic conference”. Advances in Cryptology - CRYPTO’92, Lecture notes in Computer Science, Vol. 740, 471-486, Springer-Verlog, New York, 1992.

[6] S. Akhbarifar and A. M. Rahmani, “A Survey on key pre-distribution Schemes for security in Wireless Sensor Networks”. International Journal of Computer Networks and Communications Security, Vol. 2, No. 12, 423–442, Decembre 2014.

[7] A. A. Magar, “A Survey about Key Pre-distribution Scheme in Wireless Sensor Networks”, International Journal of Engineering Research and General Science, Vol. 2, Issue 6, October-November 2014.

[8] S. A. Zade and D. G. Harkut, “Key PreDistribution Model for Wireless Sensor Network”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol 4, Issue 5, May 2015.

[9] H. Chan, A. Perig and D. Song, “Random key pre distribution scheme for sensor networks”, IEEE Symposium Research in Security and Privacy, 2003.

[10] L. Zhu, Z. Zhang, J. Li and R. Zhou, “An Improved Random Key Predistribution Scheme for Wireless Sensor Networks Using Deployment Knowledge”. International Journal of Security and Its Applications Vol. 10, No. 5, pp.225-234, 2016.

[11] L.Mathew, J. K. John, T. Thomas, M. Karthik, “Three Tier Security Scheme in Wireless Sensors Networks with Mobile Sinks Using Grid”, International Journals of Advanced Research in Computers and Communication Engineering. Vol. 2, Issue 10, October 2013.

[12] Y. Xiao, V. Krishna Rayi, B. Sun, X. Du, F. Hu and M. Galloway, “A survey of key management schemes in wireless sensor networks”, Computer Communications 30, Elsevier, 2007.

[13] H. Chan and A. Perrig “PIKE: peer intermediaries for key establishment in sensor networks”, Proceedings of the 24th annual joint conference of the IEEE computer and communications societies (INFOCOM ’05), Miami, FL, USA, March 2005.

[14] D. Liu, P. Ning and W. Du, “Group-Based Key Predistribution for Wireless Sensor Networks”, ACM Transactions on Sensor Networks, Vol. 4, No. 2, Article 11, March 2008.

[15] A. Nisha and N. D. Kale, “A Survey on key Generation and Pre distribution Technique in wireless Sensors Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 2, February 2014.

[16] S. Bala, G. Sharma and A. K. Verma, “Classification of Symmetric Key Management Schemes for Wireless Sensor Networks” International Journal of Security and Its Applications Vol. 7, No. 2, March 2013.