International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 14882-14888

Sowing Seeds Protocol based Key Distribution for Wireless Sensor Network

Saif Al-Alak

Department of Computer Science, College of Science for Women, University of Babylon, Iraq.

Abstract

Wireless Sensor Network (WSN) is widely used in many life applications. WSN has many limitations in terms of energy and battery lifetime that puts constrains in implementing security protocols and key distribution. Secret key refreshment exhausts WSN energy. In this paper, a sowing seeds scheme is proposed to improve the WSN performance. The proposed protocol sows seeds to nodes once and secret keys are generated inside each node. The proposed protocol increases WSN throughput, decreases WSN energy for key distribution, and increases node performance of WSN.

Keywords: Key distribution, Network energy, Network throughput, Node performance, WSN

INTRODUCTION

Nowadays, wireless communication is used in most fields of life. Wireless communication is employed in modern civilian and military applications. Wireless Sensor Network (WSN) is one of the most important wireless communications, which is used to transfer the sensed information from nodes to a base station.

A security protocols are used to ensure data transfer safely. Furthermore, security protocols implement security algorithms for message ciphering, authentication, and integrity. The security protocol has a secret key, which is distributed among the nodes.

Moreover, the secret key should be distributed over the communicated nodes before transferring a data. Each node must have the secret key for message ciphering, and deciphering. To address this problem, a key distribution algorithm is proposed to ensure the secret key is send to a right node.

Many researchers proposed pre-distributed key protocols. Walid B. et al. in [1] proposed a key pre-distributed protocol that maps the UNITAL design to key pre-distributed. Eschenauer and Gligor in [2] proposed a Random Key Pre-distributed (RKP) protocol that adds a list of random keys to each node from a pool to be used for node identification. Chan et al. in [3] proposed a Q-composite protocol that enhances RPK scheme, where the nodes are identified when Q keys are shared. Due et al. in [4]added to RPK scheme more attributes related to its location, where it assigns a distinct pool of keys for each region. Liu and Ning in [5] proposed a protocol that pre-load the nodes with bivariate polynomials that generates a session key for nodes of common polynomial. Blom in [6] proposed a symmetric key generation protocol that provides two types of matrices: public and private secret keys matrix.

In otherwise, some researchers proposed schemes which are not based on a pre-distributed mechanism for key management in WSN. Haibing et al. in [7] proposed a key distribution protocol based on polynomial, time and identity related. Jiang and Liu in [8] proposed a key distribution protocol based on clustering model. Jilna and Jayaraj in [9] introduced an integrated architecture for key distribution in WSN based on elliptic curve cryptography. Jingjing in [10] proposed a key distribution protocol based on combined public key technique. Ali and Ki-Hyung in [11] proposed a key distribution protocol based on deploying symmetric and asymmetric key cryptography.

According to its based mechanism, key distribution algorithms are classified into two types, which are pre-distributed key likes protocols in ([12], [13], [14] and [15]), and dynamic key generation likes protocols in ([16], [17], [18], and [19]). Furthermore, in pre-distributed key algorithm the secret key is kept in the node. The security protocol would use that secret key for securing the transferred data between nodes. However, in the dynamic key generation the secret key is generated and distributed for nodes according to key distribution protocol. When the nodes agree the secret key, the security protocol uses the secret key for securing the transferred data between nodes.

The draw back in the pre-distributed key algorithm includes the inability of network to be scalable, and it has another limitation related with key refreshment. The dynamic key algorithm overcomes the network scalability and key refreshment limitations. However, dynamic key algorithm generates and distributes the secret key that means it reduces network performance.

To address the pre-distributed key and dynamic key distribution limitations, a sowing seed protocol is proposed, which distributes a seed for secret key to be generated instead of the secret key. The proposed protocol improves network performance and scalability.

PROPOSED PROTOCOL

The proposed protocol depends on snowing the seeds among nodes. The snowed seeds are used to generate secret keys. Furthermore, the base station would send seeds to nodes. Inside each node, secret keys are generated from seeds. The scenario of sending seeds to nodes is illustrated in figure 1. Each node in the network gets the same seeds to generate symmetric secret keys for securing data transmission.

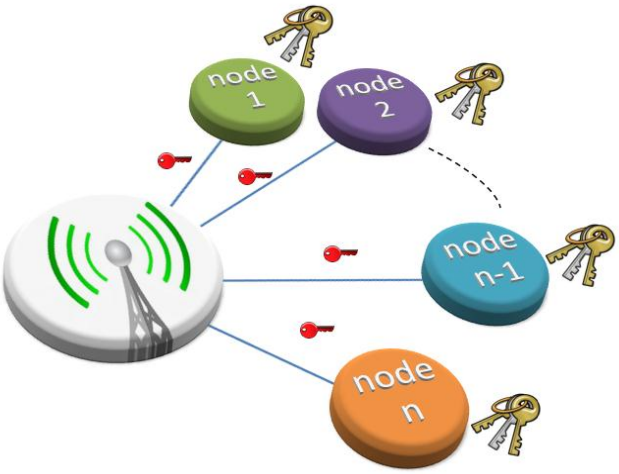

Figure 1: Proposed Key Distribution Protocol (Sowing Seeds)

Moreover, the nodes would use the seeds to generate more than one secret key. It provides multiple secret keys, which means key refreshment is possible inside each node. The generation of multiple secret keys is illustrated in figure 2. Each node receives at least two seeds (seed 1 and seed 2). When the node receives two seeds, two sets of seeds are generated from each received seed. First set is odd set that includes: (odd= {seed 1, seed 3, …, seed n-1}), and even set that includes (even = {seed 2, seed 4, …, seed n}). In each set, a new seed is generated by using a Public Key Encryption (PKE) as shown in equation 1. The secret key is generated by using a hash function (H), as pointed in Equation 2.

Seed i = PKE (Seed i-2), i > 2 Eq. 1

Where

Seed i: is new generated seed

PKE: is Public Key Encryption

Seed i-2: is previous seed

Key i = H(X, Y) , i > 0 Eq. 2

Where

Key i: is a secret key

H: is hash function

X: is seed from odd set, X = seed 2i-1, i > 0

Y: is seed from even set, Y = seed n-2(i-1), i > 0, n > 1, and n: is the number of seeds

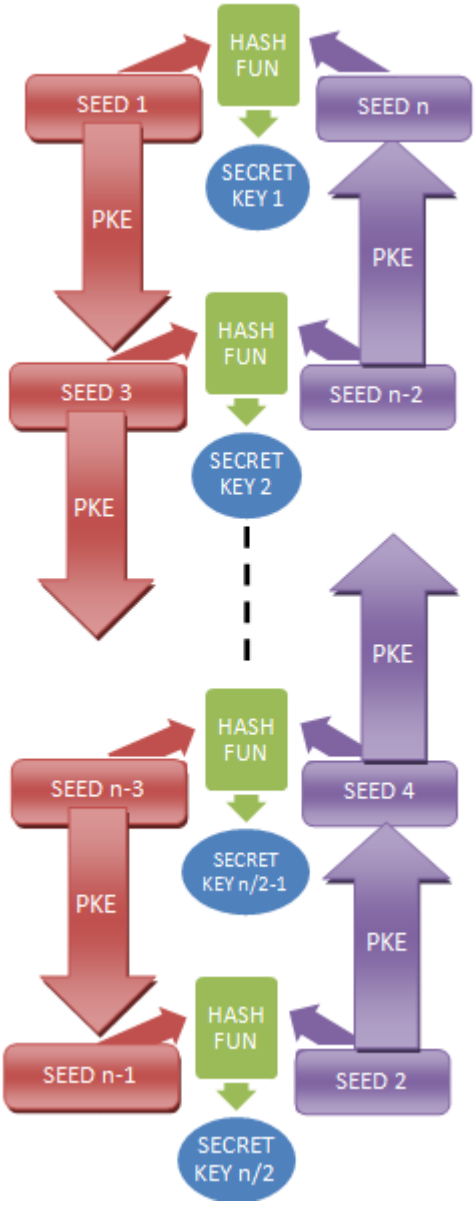

Figure 2: Secret keys generation from seeds

The number of secret keys is computed by dividing the number of generated seeds over two, since two sets of seeds is generated. Furthermore, when more than two seeds (4, 6, 8, 10 …) are received by node, the number of sets of seeds increased that leads to duplicate the number of secret key. The number of sets of seeds must be even to generate one secret key from each pair of seeds (one member from each set). The number of generated secret keys for any even number of sets of seeds is computed by dividing the number of seeds over two as shown in equation 3. The number of seeds would be divisible by the number of set of seeds. The number of seeds is a multiple of half number of sets as shown in equation 4. The sets of seeds are nominated as: odd1, odd2…odd w, even

1, even 2…even w as shown in figure 3. For any pair of seed's set (odd j, even j), the secret keys are computed in parallel with other pairs of seed's set (odd r, even r).

$K = n / 2$ Eq. 3

Where

K: is the number of secret keys

n: is the number of generated seeds

$n = i \times m, \quad i > 1$ Eq. 4

Where

n: is the number of seeds

m: is the half number of seed's sets

METHODOLOGY

The influence of the proposed protocol on the performance of WSN is measured by using NSs simulator. One of the important metrics of network performance is network throughput, which is measured in this paper. Network throughput is the amount of data transferred in a unit of time. Furthermore, node throughput is the rate of transferred data over simulation time as shown in equation 5. Network throughput is the rate of all nodes' throughput over number of nodes as shown in equation 6. The simulator's parameters are set as illustrated in figure 4.

$S\_Node = D/T$ Eq. 5

Where

S_Node: node's throughput

D: amount of transferred data

T: simulation time

$S\_Net = \sum S\_Node\ i / N\_Node, \quad N\_Node \leq i \geq 1$ Eq. 6

Where

S_Net: network throughput

S_Node: node's throughput

N_Node: number of nodes

The energy consumption of a node is measured by computing the metric Percent Consumed Energy (PCE). The Consumed Energy (CE) of a node is computed by equation 7. PCE is a percent of consumed energy to initial energy as shown in equation 8. The average PCE for all nodes is computed by equation 9.

$CE = InitialEnergy - FinalEnergy$ Eq. 7

Where

CE: is a node's consumed energy

$PCE = CE / InitialEnergy \times 100\%$ Eq. 8

Where

PCE: is a node's percent consumed energy

CE: is a node's consumed energy

$APCE = \sum PCE\ i / N\_Node, \quad N\_Node \leq i \geq 1$ Eq. 9

Where

APCE: is an average of nodes' percent consumed energy

PCE: is a node's percent consumed energy

N_Node: number of nodes

Odd 1	Even 1	Odd 2	Even 2	…	Odd w	Even w
Seed 1	Seed 2	Seed 3	Seed 4		Seed m-1	Seed m
.	.	.	.		.	.
.	.	.	.		.	.
.	.	.	.		.	.
Seed n-m+1	Seed n-m+2	Seed n-m+3	Seed n-m+4	…	Seed n-1	Seed n

Figure 3: Seed's Sets

radio-propagation model	Propagation/TwoRayGround
Mac/802_15_4	Phy/WirelessPhy/802_15_4
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/OmniAntenna
max packet in queue	150
routing protocol	AODV
traffic type	CBR
Nodes	15
Node location	circle
Packet Size	70
Pt	0dBm(1mW)
RxThresh	-97dBm, -92dBm, -87dBm, -82dBm
CSThresh	-97dBm
CPThresh	10
Antenna Hight	1.0m
txPower	0.0744W
rxPower	0.0648W
idlePower	0.00000552W

Figure 4: Parameters of Network Simulation

Four states are tested to measure the influence of the proposed key distribution protocol on network throughput of WSN. Moreover, in each state 30 different data rate are tested (0.1, 0.2…2.9, 3) kb/s. The secret key is refreshed after sending (50, 100, 150, and 200) packets in first, second, third, and fourth state consequently.

RESULT AND DISCUSSION

The proposed protocol improves network throughput, node's consumed energy, and node performance. Furthermore, the proposed protocol reduces the amount of data for key distribution. Since the WSN needs to refresh the secret key, the base station distributes a fresh secret key every time. However, the proposed protocol improves the network throughput by distributing seeds that are used to generate secret keys instead of distributing the secret keys themselves.

The propose protocol provides a random way to generate secret keys from seeds that ensure a difficulty to regenerate the secret keys from attackers. The secret keys are generated in parallel to improve node performance.

i. Network Throughput

The network throughput is increased when the proposed protocol is used. (S1) is a network throughput of a network that is based on seed distribution (propped protocol). (S1) is higher (better) than network throughput (S2, S3, S4, and S5). (S2, S3, S4, and S5) are network throughput of networks that are based on secret key distribution as illustrated in figure 5 a (state 1), b (state 2), c (state 3), and d (state 4).

Furthermore, when secret keys are refreshed in the network after sending (200) packets, the network throughput (S2) is less than (S1). When secret keys are refreshed after sending (150, 100, and 50) packets (more security), the network throughput (S3), (S4) and (S5) for key distribution based network is less than throughput (S1) for seed distribution (proposed protocol) based network as illustrated in figure 5 a (state 1), b (state 2), c (state 3), and d (state 4).

The proposed protocol improves the network throughput by reducing the number of transferred secret keys. The secret keys are distributed through packets in the network. When the proposed protocol is used, data packets are sent in the network instead of secret keys packets.

ii. Energy for data transfer

Energy consumption is one of the limitations in WSN. The transferring of data over WSN consumed sensor energy. For transferring an amount of data over the wireless network, each transferred packet consumed a sensor's energy during sending and receiving a packet. The using of secret key for ciphering a transferred data leads to secret key refreshing, which means consumed more energy during key refreshing.

The average percent consumed energy (APCE) is computed for the network. When secret key is refreshed after sending (200, 150, 100, and 50) data packets, the average percent

consumed energy is (APCE 2, APCE 3, APCE 4, and APCE 5) respectively. For secure data transfer in WSN, the proposed protocol has less network consumed energy (APCE 1) in compare to network consumed energy (APCE 2, APCE 3, APCE 4, and APCE 5) when secret key is refreshed after sending (200, 150, 100, and 50) data packets respectively as illustrated in figure 6.

When the proposed protocol is used, the number of transferred packets would be reduced because the proposed protocol does not need to refresh the secret key, which means the proposed protocol reduces the consumed energy. Moreover, the secret key is distributed through its seeds without needing to key refreshing. Furthermore, the proposed protocol saves the sensor energy

iii. Node Performance

Most of the WSN devices are support parallel implementation for security protocol. The proposed protocol provides multiple secret keys, which enables the node to implement the security protocols in parallel. Furthermore, the parallel implementation of security protocols increases its implementing rate. When (2, 4, 8…) seeds are provides to node, the security protocols implementation increases about (50%, 75%, 83% ...) consequently, as illustrated in figure 7. The increasing of the number of seeds improves (increases) the implementation speed of security protocols for a node.

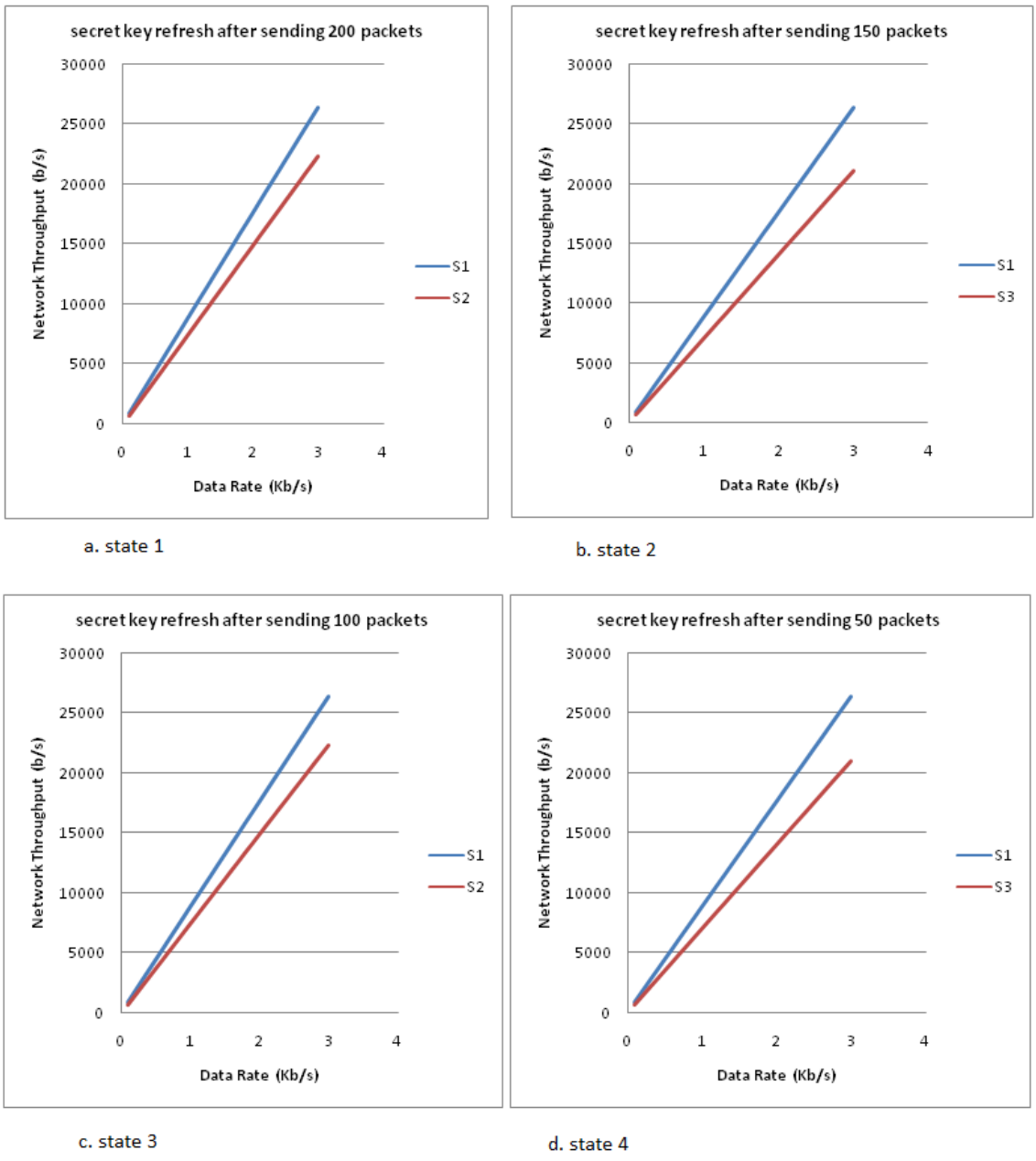

Figure 5: Network Throughput

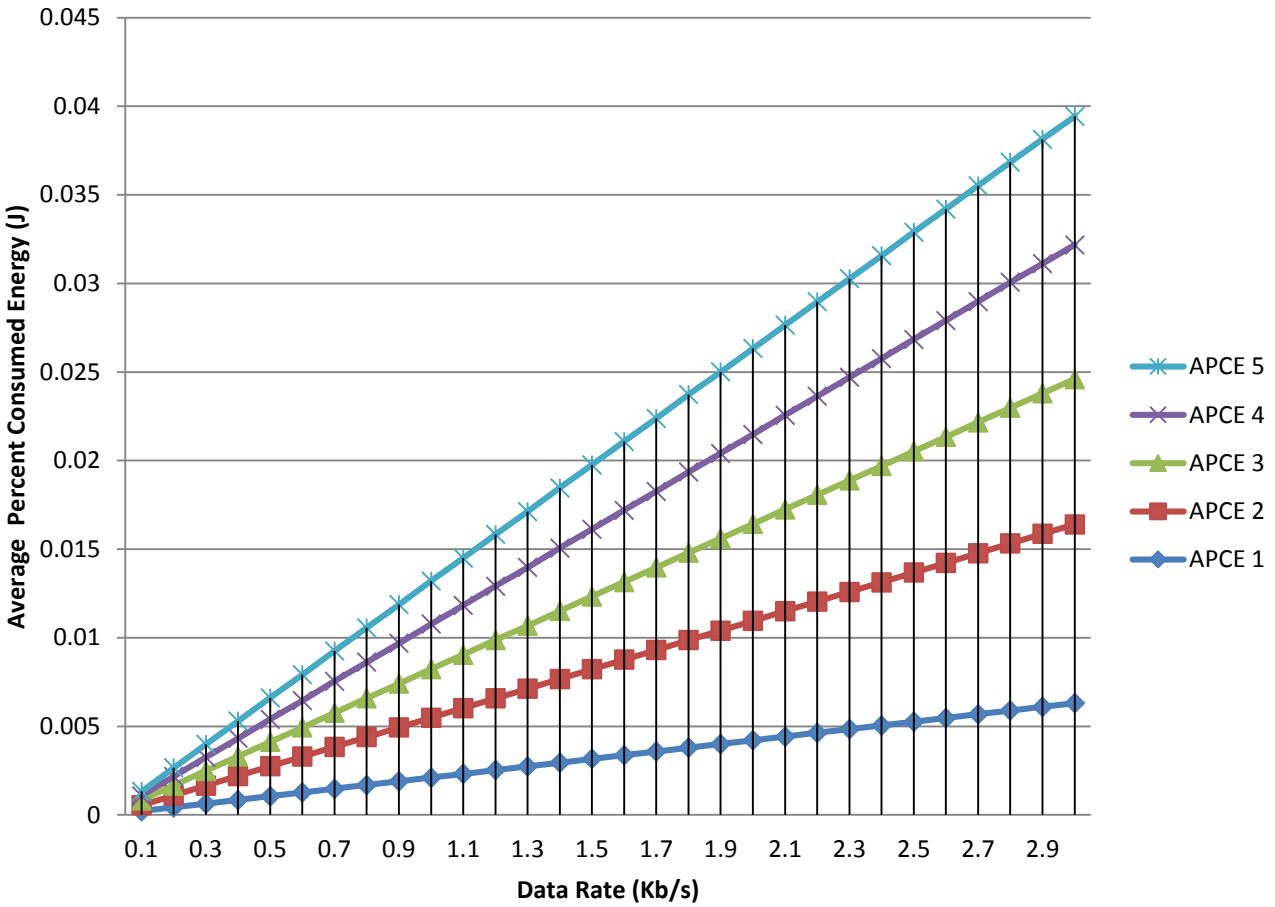

Figure 6: Transferred Data Energy

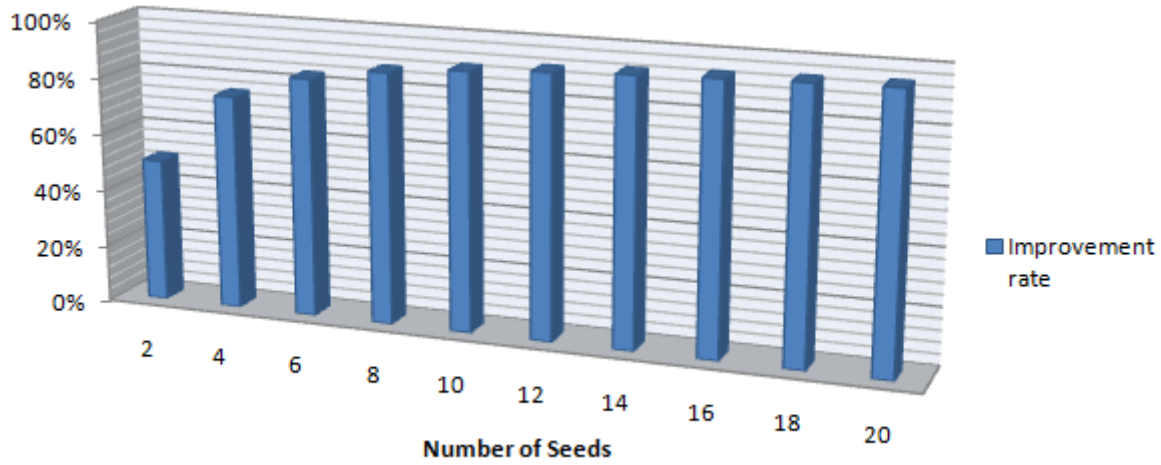

Figure 7: Improvement Rate of Security Protocols Implementation

CONCLUSION

WSN has many limitations in terms of energy and battery lifetime. The implementing of security protocol likes key distribution reduces WSN performance. A sowing seeds scheme is proposed to improve the WSN performance. The proposed scheme distributes seeds to nodes once; secret keys are generated inside each node without needing for key refreshing. The using of proposed protocol leads to increase

throughput, and node performance of WSN. The energy for key distribution is decreased.

REFERENCES

[1] Bechkit, W., Y. Challal, and A. Bouabdallah. *A new scalable key pre-distribution scheme for wsn*. in *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*. 2012: IEEE.

[2] Eschenauer, L. and V.D. Gligor, *A key-management scheme for distributed sensor networks*, in *Proceedings of the 9th ACM conference on Computer and communications security*. 2002, ACM: Washington, DC, USA. p. 41-47.

[3] Chan, H., A. Perrig, and D. Song. *Random key predistribution schemes for sensor networks*. in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. 2003: IEEE.

[4] Du, W., et al. *A key management scheme for wireless sensor networks using deployment knowledge*. in *INFOCOM 2004. Twenty-third AnnualJoint conference of the IEEE computer and communications societies*. 2004: IEEE.

[5] Liu, D., P. Ning, and R. Li, *Establishing pairwise keys in distributed sensor networks.* ACM Transactions on Information and System Security (TISSEC), 2005. **8**(1): p. 41-77.

[6] Blom, R. *An optimal class of symmetric key generation systems*. in *Workshop on the Theory and Application of of Cryptographic Techniques*. 1984: Springer.

[7] Haibing, W., et al. *WSN key distribution method based on PTPP*. in *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on*. 2014: IEEE.

[8] Jian-wei, J. and L. Jian-hui. *Research on key management scheme for wsn based on elliptic curve cryptosystem*. in *Networked Digital Technologies, 2009. NDT'09. First International Conference on*. 2009: IEEE.

[9] Jilna, P., P. Deepthi, and U. Jayaraj. *Optimized hardware design and implementation of EC based key management scheme for WSN*. in *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for*. 2015: IEEE.

[10] Li, J., L. Tan, and D. Long. *A new key management and authentication method for WSN based on CPK*. in *Computing, Communication, Control, and Management, 2008. CCCM'08. ISECS International Colloquium on*. 2008: IEEE.

[11] Tufail, A. and K.-H. Kim. *A backbone assisted hybrid key management scheme for WSN*. in *Information Society (i-Society), 2011 International Conference on*. 2011: IEEE.

[12] Di Pietro, R., L.V. Mancini, and A. Mei. *Random key-assignment for secure wireless sensor networks*. in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. 2003: ACM.

[13] David, H., C. Bo-Cheng, and V. Ingrid, *Energy-memory-security tradeoffs in distributed senor networks.* Proc InternationalConference on Adhoc Networks and Wireless (ADHOC-Now2004). German: Springer Berlin/Heidelberg, 2004. **70281**.

[14] Yuan, Q., et al., *Optimization of key predistribution protocol based on supernetworks theory in heterogeneous WSN.* Tsinghua Science and Technology, 2016. **21**(3): p. 333-343.

[15] Derashri, K., N. Chaudhary, and K. Jain, *A Survey on Key Pre-Distribution in WSN.* International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017. **2**(3).

[16] Lai, B., S. Kim, and I. Verbauwhede. *Scalable session key construction protocol for wireless sensor networks*. in *IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)*. 2002.

[17] Dutertre, B., S. Cheung, and J. Levy, *Lightweight key management in wireless sensor networks by leveraging initial trust*. 2004, Technical Report SRI-SDL-04-02, SRI International.

[18] Singh, A., A.K. Awasthi, and K. Singh. *Lightweight multilevel key management scheme for large scale wireless sensor network*. in *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*. 2016: IEEE.

[19] Mall, D., K. Konaté, and A.-S.K. Pathan. *ECL-EKM: An enhanced Certificateless Effective Key Management protocol for dynamic WSN*. in *Networking, Systems and Security (NSysS), 2017 International Conference on*. 2017: IEEE.