ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

AN EFFICACY HYBRID KEY PRE-DISTRIBUTION SCHEME FOR WIRELESS SENSOR NETWORK

R. Chitra, M.Sc.,(Maths), PGDCA, B.Ed., M.Sc., IT., M.Phil (CS)
Assistant Professor, Department of Computer Science, MCA and IT & Applications,
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

G. Kayalvizhi
Research Scholar, Department of Computer Science
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

Abstract

Most of the key management schemes do not consider the attacking behavior of the adversary makingsuch schemes less practical in real world. By knowing the adversarial behavior, several countermeasuresagainst them can be effectively and efficiently designed by the defender/network designer. In this paper, the investigation in the problem of compromise link and propose a secure hybrid key pre-distribution scheme (HKPS) for wireless sensor networks (WSN).This scheme combines the robustness of the q-composite scheme with threshold resistant polynomial scheme. The proposed scheme aims to make the network more resistant against the node capture attacks.

Keywords: Key Pre-distribution, Wireless Sensor Network, Security Services, Attack probability, q-Composite scheme, Resilience against node capture,Key connectivity, Random key pre-distribution scheme

1. Introduction

Wireless sensor network (WSN) comprises of small resource constrained sensors that actively monitor their surroundings, collectthe data and send it to the central authority. The centralauthority is the base station (BS) that acts as a powerful data processingand storage center [1]. The sensors havelimited energy and processing power that makes the heavy weightpublic key encryption infeasible solution for WSN security.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Thesecurity mechanisms should be lightweight and energy efficientfor WSN. Duty cycled WSNs in which sensor are sleep and awakeat some interval of time is one such technique to reduce the energyconsumption during query processing [2].Location based sleep scheduling is another technique to improve the energy efficiency of WSN integrated with mobile cloud computing [2]. As the sensors have limited resources and deployed in the hostile environments, WSNs are susceptible to various attacks. One such attack is the node capture attack. The resistance of key management scheme (KMS) against this attack emerges an important and challenging issue in WSN security. The WSN security resides in securing the keys used for encryptingthe data [3] [4].Therefore, the fundamental question is how to design a secure aKMS that guarantees the proper functionality of WSN services even in the presence of the adversary[5]. WSNs have applications in diverse domains such as defense, medical care, environmental monitoring, disaster management, inventorycontrol etc. KMS is the set of processes that facilitate the secure transmission of data between sensor nodes [6].

Due to wireless nature of communication channel, there are many inherent security issues such as eavesdropping, forgeryattacks, off-line guessing attacksetc in WSN. These networks are often deployed in unattended, hostile and critical environments, thus there is a need for effective and efficient techniques to fulfill the security requirements. Key establishment schemes aim to provide pair-wise keys among the neighboring nodes to support ongoing relationship in a network. But it becomes complicated due to the limited computational power, battery power and storage capacity of sensor nodes. Most of the KMS assumes that every node of the network has same probability of attack. This assumption may not be true for many WSN applications such as military and border surveillance making these schemes less practical in real world environments. Can we develop mechanisms that both resilience and connectivity of key pre-distribution schemes increases? It was also pointed that ‘‘a system without adversary definition cannot be secure. It can only be astonishing” by [7]. It states that defensive mechanisms should be designed after analyzing the adversary behavior. Had there been a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

reliable, secure and realistic designed KMS for WSNs, an attack such as node capture would not be able to degrade the performance of KMS to such an extent. Motivated by this fact, this paper presents an attack resistant key pre-distribution that combines the strong points of the q-composite with the polynomial scheme to make the network more secure against node capture.

2. Literature Survey

Due to their inherent properties, WSNs are susceptible to various attacks. These attacks break the confidentiality, integrity andavailability of the network. Such attacks can be classified as passive and active attacks. The listening of communication channels byunauthorized users is the passive attacks such as eavesdropping,traffic analysis and passive monitoring. These attacks breach theconfidentiality and privacy of the network data. The active attacks falsify, modify, listen, monitor the data packets in the network. The common active attacks are camouflage, sybil, wormhole, replay, hello flood, sink hole, denial of service, and node replication. Sink is the most trusted component of the WSN and cannot be compromised by the adversary. It acts as a gateway to forward the collected data to some external environment and thus, sink holenode detection becomes an important in WSN security [8]. Even some attacks such as black hole are difficult to detect and defend and thus, their timely detection and prevention is crucial in the network security [9]. Authentication also is an important aspect of security as it allows the authorized access to information available through sensor nodes [10].

In this paper, we focus on the key distribution schemes in WSN security. KMS plays a very significant role by establishing secure communication among the sensor nodes. In 2002, [5] proposed random key pre-distribution scheme for WSNs. This scheme is also called EG scheme or the basic scheme. It has three phases - key pre-distribution, discovery of shared key and establishment of path key. The keys are assigned from a large key pool. If the nodes are not able to find a common key, they perform path key establishment with intermediate nodes. EG scheme was further strengthened by the q-composite scheme where the nodes have to share q keys instead of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

one key [11]. This increases safety of the scheme. Deployment based key management scheme is given [12] in which the neighboring nodes share more number of keys than non-neighboring nodes in a network. The requirement of prior deployment information limits the practical use of such schemes. Authors [6] present a secure scheme by considering threats that may occur inside the network. A polynomial pool scheme is proposed [13] that uses bivariate polynomials to establish the pair-wise key. This scheme suffers from large storage overhead but has high security in small scale attacks. The polynomial scheme has t-threshold property which states that the scheme is not compromised if the number of captured nodes is less than t. In recent researches, many scholars have presented a combined approach that combines the advantages of two different schemes with limited complexity. Authors [14]proposed in [15]presented a hash based key pre-distribution scheme for WSN. Thehash function is used to conceal the pre-distributed keys from an adversary. It is shown that this scheme has increased resistance against node capture. An unbalanced key distribution scheme is proposed in [12] that assign larger key ring size to high end sensors and minimum key ring size to low end sensors. This increases the overall performance of KMS.

3. Proposed Hybrid Key Pre-distribution Scheme

Initially, an attack matrix is constructed by the networkdesigner or defender by considering different vulnerabilities. This matrix is constructed by considering the view point of adversary and is done at the time of deployment of the nodes in the network. An adversary has full information of the network topology, route information and key identifier information [16] [17] [18] [19]. This matrix is used to formalize an attack and a set of captured candidate nodes is computed. The nodes of the network are classified into vulnerable and safe nodes. The vulnerable nodes are assigned smaller key ring size as compared to safe nodes. This increases the resistance of the proposed scheme as the chances of key compromise are reduced due to small number of stored keys. The smaller key ring size reduces the leakage of the keying information to the adversary. The attack coefficient of a node is used to perform hash chaining on its pre-distributed keys.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Table 1: Algorithm Notation and its meaning

Notation	Meaning
N	Total nodes of the network
C	Set of cut vertex node
K_j	Keys contained by j^{th}node
AAC_i	Application attack coefficient of ith node
S	Set of sink nodes
ac_i	Attack coefficient of ith node
CC_i	Capturing cost of ith node
C_n	Set of compromised nodes
C_k	Set of compromised keys
ID_v	Node identifier
M	Key ring size
P	Key pool
L	Limit parameter
N	Polynomial shares
P	Polynomial pool
CVD	Matrix based on Cut Vertex
AC_CVD	attack coefficient of a nodes based CVD matrix
CVP	cut vertex partial compromise matrix
AC_CVP	attack coefficient based CVP matrix
SD	matrix based on the direct sink key compromise
AC_SD	attack coefficients of the nodes based on the sink node
SP	partial compromise of the nodes with sink node
AC_SP	attack coefficient based on SP
A_CD	attack coefficient based on direct compromise

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

CP	attack coefficient based on partial compromise
AC_D	attack coefficient based on direct compromise
AC_P	attack coefficient based on partial compromise
F'AC	final value of the attack coefficient of the node based on the capturing cost
CC	Cost of capturing a sensor node
cmd	relative importance of the direct compromise over partial compromise
d	number of sink nodes
k	hop distance from the sink
lp	limit parameter
sk_t	the number of sub key pools
skp_k	each sub key pool has number of keys
v	sub key pool of a node
$ID_{Kp(v)}$	each key with a subkey pool identifier list

Algorithm: Hybrid Key Pre-distribution Scheme

Step 1:Method 1: To compute attack coefficient of a node based on node dominance (AC-ND)

Step 1.1: Input: N, K, S, SR

Step 1.2: Output: DC, PC

Step 1.3: for all $n_i \in$ N-(S + SR)

Step 1.4: for all $n_j \in$ N-(S + SR)

Step 1.5: if n_i can directly compromise $n_j dc_{ni}^{++}$

Step 1.6: else if n_i can partially compromise $n_j pc_{ni}^{++}$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Step 1.7: end if

Step 1.8: end if

Step 1.9: end for

Step 1.10: end for

Step 1.11: end for

Step 1.12: return DC and PC // Return the attack coefficient of a node

Step 2: Method 2: To identify the set of candidate capture node based on estimated value of F'AC

Step 2.1. Input: AC_D, AC_P, cmd

Step 2.2. Output: C_n and C_k/*C_n is the set of compromised nodes and $C_k$is the set of compromised keys*//*

Step 2.3: Construct FAC

Step 2.4: Construct CC

Step 2.5: Construct F'AC

Step 2.6: while all routing paths are destroyed do

Step 2.7: Find $n_i \in V$ such that it has maximum attack coefficient i.e. $C_n \in$ arg max (F'AC)

Step 2.8: Select n_i, $C_n = C_n \cup n_i$, $C_k = C_k \cup k_i$

Step 2.9: Adjust F'AC

Step 2.10: end while

Step 2.11: return C_n and C_k

Step 3: Method 3: To assign a random keys to the nodes in the proposed scheme.

Step 3.1: Input: ID_v ,. . .,$ID_{Kr(v)}$; $ac_{(u)}$, Hash function, lp

Step 3.2: Output$ID_{Kr(v)}$, KP(v) KDS randomly group the keys into sk_tkey pools where each sub key pool has skp_k keys

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

*Step 3.3:*KDS assigns sk_n key pool to each node of the network

*Step 3.4:*r number of keys from each sub key pool are randomly assigned to the nodes

*Step 3.5:*For $n_i \in N$ $kr_i = \{hash^{acimodlp}(k_1), hash^{acimodlp}(k_2) \ldots hash^{acimodlp}(k_r)\}$

*Step 3.6:*return $ID_{Kr(v)}$, KP(v)

4. Performance Analysis of the proposed Hybrid Key Pre-distribution scheme

4.1 Polynomial and Key connectivity

Key connectivity is the probability that two nodes in the range of communication have common key. We find that the key connectivity remains the same even if we store less number of keys in vulnerable nodes in HKP scheme as shown in Fig. 1. The relationship between the polynomial rings of the two pre-distribution schemes is M x N = x^2. We also observe that even if small number of the polynomial shares is stored in vulnerable nodes of the proposed scheme, the key connectivity remains unchanged and is same as in balanced distribution. This is due to the fact that total polynomial shares remain same in both schemes. This proves the effectiveness of the proposed scheme in terms of improved security without affecting the key connectivity. We also observe that with increase in polynomial size, the key connectivity decreases. To plot this figure, we have taken the following values: key ring size ofnodes in balanced key pre-distribution-s= [2, 4], key ring size ofsafe nodes in proposed scheme-m = [4, 8] and key ring size of vulnerablenodes in proposed scheme-n = [1, 2].

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

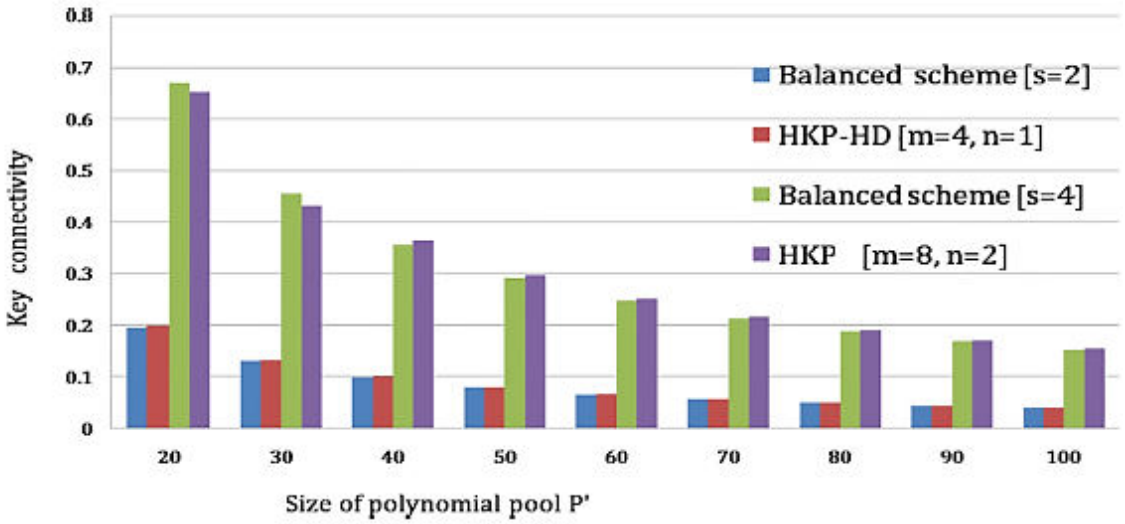

Figure 1: The relationship between the polynomial pool size and the key connectivity

4.2 Probability of key compromise

It is shown in Figure 2 that the HKPS has least probability of key compromise as compared to other existing schemes. Du is unbalanced key pre-distribution where PPBR is the combination of polynomial pool with key pool scheme. In PPBR, size of key ring is obviously lesser than Du scheme. Thus, in PPBR key ring size gets reduced which results in smaller value of probability of key compromise than Du scheme. The proposed HKP-HD has even lesser probability of key compromise than PPBR. It is due to incorporation of hash chain pre-distribution with multiple sub key pools. Thus,proposed HKP scheme further reduces the key compromise probability of PPBR scheme. From Fig. 2(a), 2(b) and 2(c) that when increase the value of q, the probability of key compromise gets decreased in proposed HKP-HD. This is due to the fact that key overlapping increases with increase in q. This leads to increase in the number of captured nodes to break the link keys. The hash based pre-distribution of the proposed scheme decreases the probability of key compromise and hence, the number of effected nodes during node capture also gets decreased. This furtherincreases resistance of the scheme against node capture.When the number of captured nodes reaches to 100, probabilityof key

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

compromise almost reaches to one as value of variable t is taken 100. To plot the graph, the following values are taken to plot the graph: S = 1000, t = 100, m = 40, P0 = 14, n = 5, lp = 10.

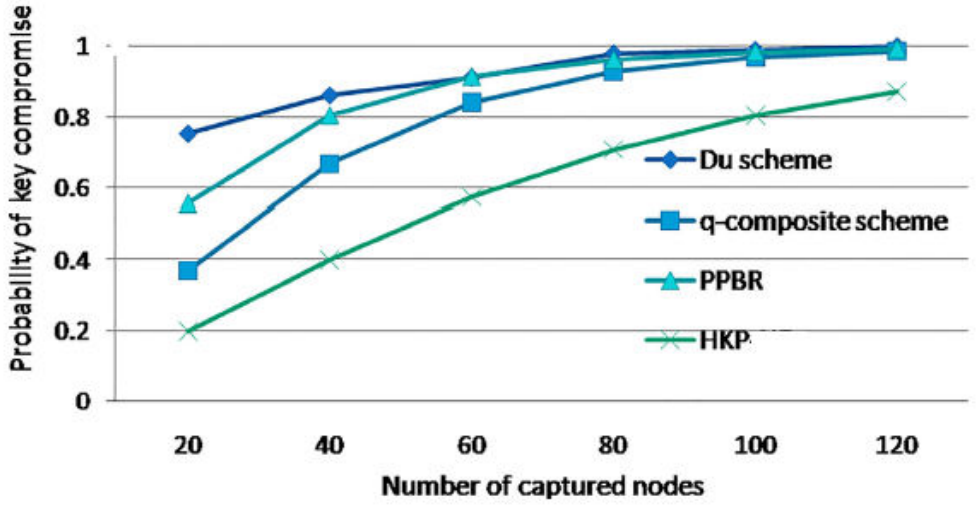

Figure 2a: Probability of key compromise for number of captured nodes with q=1

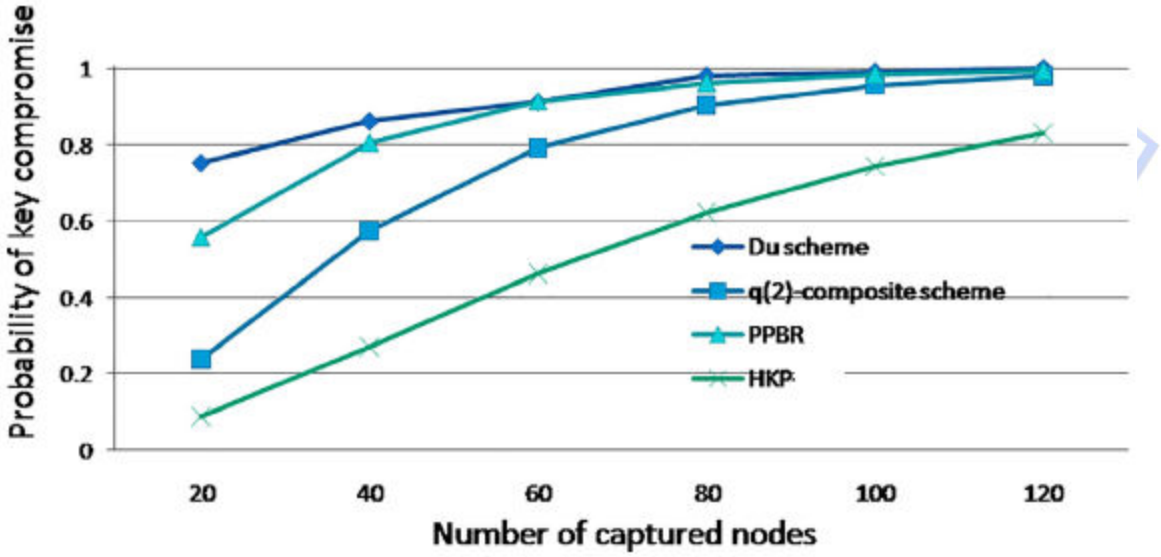

Figure 2b: Probability of key compromise for number of captured nodes with q=2

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

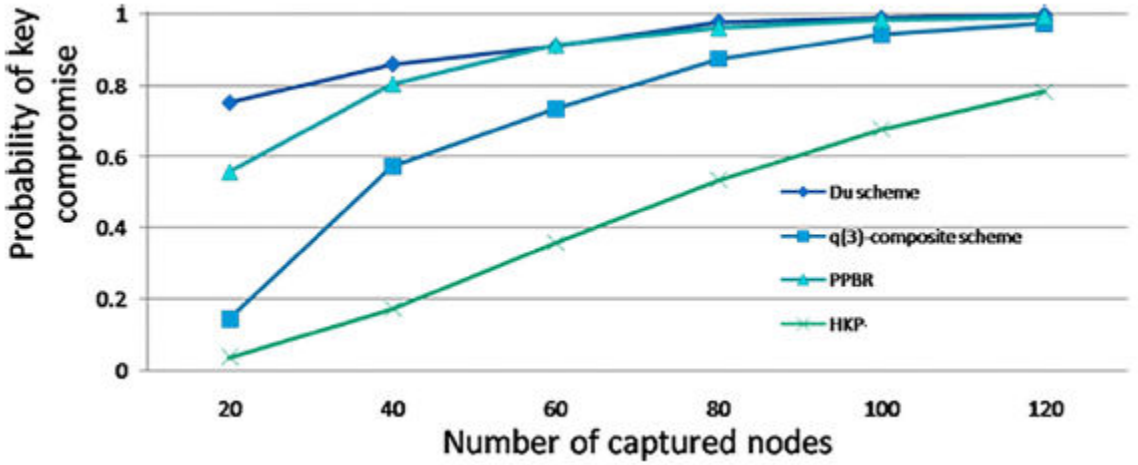

Figure 2c: Probability of key compromise for number of captured nodes with q=3

4.3 Communication overhead

Fig. 3(a) and 3(b) depict that HKP scheme has least value of communication overhead as compared to Du scheme. HKP scheme divides thedomain key pool into multiple sub key pools. In HKP scheme, the sharedkey is discovered in two stages. In the first stage, the sub key poolidentifiers are transmitted over a network. The second stage is initializedonly when there are common key pool identifiers betweenthe communicating nodes. The node transmits the key identifiers ofcommon sub key pools in second stage of key discovery. In Duscheme, the key identifiers are compared during shared key discovery.This results in large number of key comparisons and thus, haslarger value of communication overhead as compared to HKP scheme.If we increase the size of key pool, the communication overheadincreases at a greater rate in Du scheme than in proposed scheme.The same is true for increase in key ring size also.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

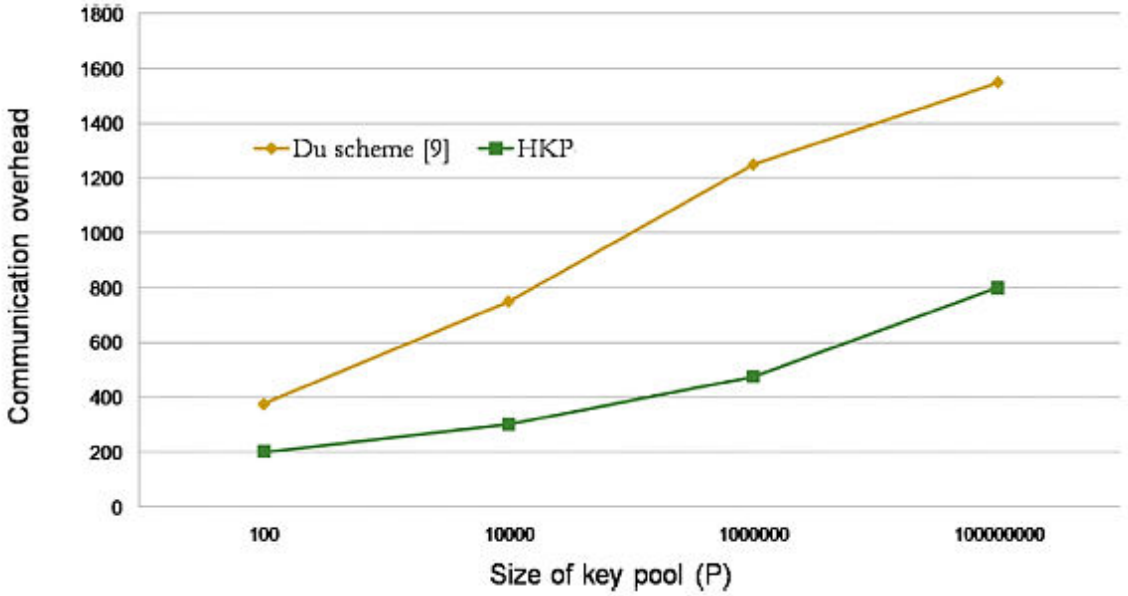

Figure 3a: Comparison of the communication overhead with k_{spn}>2

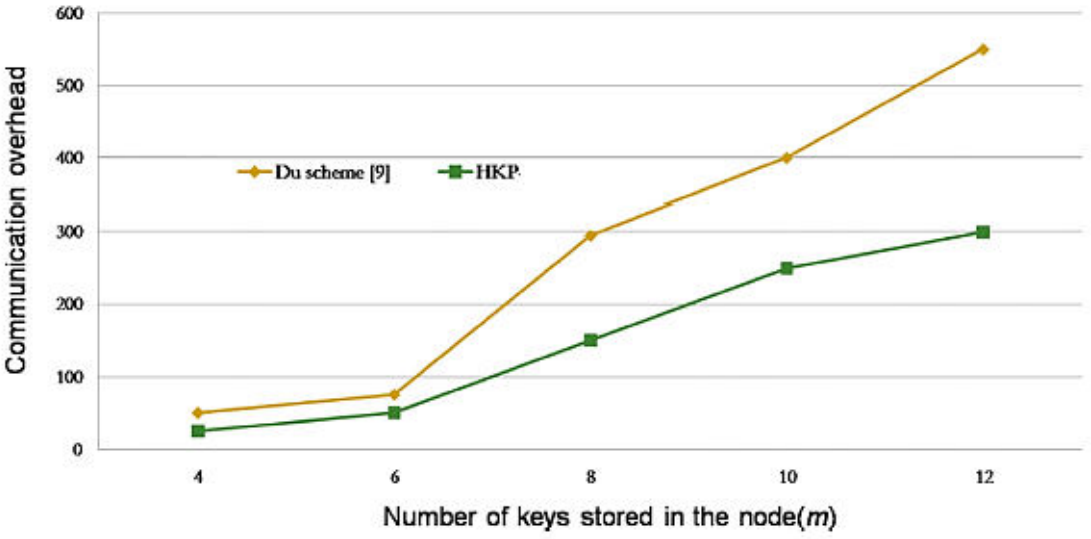

Figure 3b: Comparison of the communication overhead with k_{spn} =2

5. Conclusion

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

This paper presents an attack resistant key pre-distribution (HKP) that combines robustness of the q-composite scheme withunconditional secrecy of the polynomial pool scheme. The proposedscheme aims to reduce the communication overhead and probability of key compromise without degrading its key connectivity. The hash chain with multiple sub key pools of the proposed scheme has reduced the probability of the key compromise and communication overhead. The unbalanced key pre-distribution of the proposed scheme further decreases the storage overhead on the vulnerable nodes of the network without sacrificing the key connectivity. It increases the resistance of the proposed scheme against node capture. To design the solution of isolation of vulnerable nodes in the network and energy consumption of proposed scheme are proposed as the future work. The future plan is to find the optimal values of the variables-cmd, lp and AAC.

Reference

[1] Aikyildiz, I.F., Su, W., Sankarasubramaniam, Cayir, E., 2002. Wireless sensor networks: a survey. Comput.Netw. 38 (4), 393–422.

[2] Zhu, C., Yang, L.T., Shu, L., Leung, V.C., Hara, T., Nishio, S., 2015a. Insights of top-$ k $ query in duty-cycled wireless sensor networks. IEEE Trans. Ind. Electron. 62 (2), 1317–1328.

[3] Zhang, J., Varadharaja, 2010. Wireless sensor network key management survey and taxonomy. J. Netw. Comput. Appl., 63–75.

[4] Bhushan, B., Sahoo, G., 2017. Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wireless Pers. Commun., 1–41.

[5] Eschenauer, L., Gligor, V., 2002. A key-management scheme for distributed sensor networks. In: Proceedings of 9th ACM Conference on Computer and Communications Security, pp. 41–47.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

[6] Choi, J., Bang, J., Kim, L., Ahn, M., Kwon, T., 2017. Location-based key management strong against insider threats in wireless sensor networks. IEEE Syst. J. 11 (2), 494–502.

[7] Gligor, V.D., 2008. Handling new adversaries in wireless ad-hoc networks (transcript of discussion). In: International Workshop on Security Protocols. Springer, Berlin, Heidelberg, pp. 120–125.

[8] Wazid, M., Das, A.K., Kumari, S., Khan, M.K., 2016. Design of sinkhole node detection mechanism for hierarchical wireless sensor networks.Secur.Commun.Netw. 9, 4596–4614.

[9] Wazid, M., Das, A.K., 2017. A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. Wireless Pers. Commun. 94 (3), 1165–1191.

[10] Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K.K.R., Das, A.K., 2016. An efficientauthentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. J. Netw. Comput.Appl.

[11] Chan, H., Perrig, A., Song, D., 2003. Random key predistribution schemes for sensor networks'. In: Proceedings of 2003 IEEE Symposium on Security and Privacy. California, USA, pp. 197–213.

[12] Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K., 2004. A key management scheme for wireless sensor networks using deployment knowledge. In: INFOCOM 2004. Twenty-third Annual Joint conference of the IEEE computer and communications societies. IEEE, pp. 586–597.

[13] Ling, D., Ning, P., Du, W., 2008. Group based key pre-distribution for wireless sensor networks. ACM Trans. Sensor Netw. TOSN, 11–18.

[14] Bechkit, W., Challal, Y., Bouadallah, A., 2013. A new class of hash chain based key predistribution scheme for WSN. Comput.Commun. 36, 243–255.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

[15] Zhang, J., Cui, Q., Yang, R., 2016b. A Hybrid key establishment scheme for wireless sensor networks. Int. J. Secur. Appl. 10 (2), 411–422.

[16] Lin, C., Wu, G., Qiu, T., Deng, J., 2015. A low cost node capture algorithm for wireless sensor networks. Int. J. Commun. Syst. https://doi.org/10.1002/dac.3097.

[17] Chen, X., Makki, K., Yen, K., Pissinou, N., 2007. Attack distribution modeling and its applications in sensor network security.EURASIP J. Wireless Commun.Netw.,1–11.

[18] Yu, C.-M., Li, C.-C., Lu, C.-S., Kuo, S.-Y., 2011. An application driven attack probability based deterministic pair-wise key pre-distribution scheme for non-uniformly deployed sensor networks. Int. J. Sensor Netw. 9 (2), 89–106.

[19] Ahlawat, P., Dave, M., 2016. An improved hybrid key management scheme for wireless sensor networks. In: Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on, pp. 253–258.