A Hash Key-Based Key Management Mechanism for Cluster-Based Wireless Sensor Network

Sachin D. Babar and Parikshit N. Mahalle

Sinhgad Techincal Education Society, Pune, Maharashtra, India
E-mail: sdbabar@sinhgad.edu; aalborg.pnm@gmail.com

Received 2 July 2016; Accepted 9 January 2017;
Publication 27 January 2017

Abstract

The growth of wireless sensor networks (WSNs) in the last few years, enhances the use, efficiency, and accuracy of a large number of applications such as defense, habitat monitoring, industrial, and many more. The performance of WSN is largely affected by the security, as large numbers of security attack are happening on the WSN. Therefore, it is necessary to have a security solution to use the WSN proficiently. The objective of this paper is to address the security problem of WSN by proposing the key management mechanism to establish the secure link for communication. The paper proposes the cluster-based key management technique based on hash key mechanism. The mechanism considers the key establishment and verification at two levels, one at one-hop distance and the other at multi-hop destination. The proposed work is evaluated by considering the varying number of attackers in the network. The mechanism shows reduced packet lost rate and energy consumption as compared with one-hop key management solutions, by making the tradeoff of delay. The results shows the improvement in packet loss rate i.e., without any solution, if attack happens obviously the attack performance reduces with an increase in pack loss rate and after applying the solution, the packet loss rate is reduced.

Journal of Cyber Security, Vol. 5_2, 73–88.
doi: 10.13052/jcsm2245-1439.524

Keywords: Wireless sensor network (WSNs), security, cluster-based, key management, hash key.

1 Introduction

WSN is a network of small, miniature sensor nodes, which communicate with each other to achieve common tasks. The work of such a network is to collect sensed information from different sensor nodes and communicate it to sink node.

The applications of WSN are spreading in many different domains, such as military, habitat monitoring, vehicle network, telemedicine, and many more. The use of WSN in such real time applications produces the security requirements to the WSN application. Hence security is important in WSN to save it from malicious attacks [1, 2].

WSN is subject to different kind of denial of service (DoS) attacks, e.g. jamming attack. This attack degrades the performance by jamming the channel or by denying the channel service [3–5]. The key management mechanisms are playing major roles to defend such attacks. The literature [6–10] proposes different key management algorithms considering network management and sharing of key among the different nodes. The key management mechanisms available for establishing secure connectivity must minimally incorporate authenticity, confidentiality, integrity, scalability, and flexibility [6–10]. The work considered here focuses on hash-based key management mechanism. Hash-based key management mechanism is shown to be an important and applicable security solution for WSN. The current hash-based key management mechanisms [6–10] are efficient, but they are complex leading to an increase in overheads. They are not scalable and adaptable based on the situations of ad-hoc networks.

Nowadays most of the WSN deployments are made using cluster-based networks for improving energy efficiency and scalability. Therefore, it is necessary to develop a defense mechanism by considering cluster-based networks with efficient key management mechanisms. The paper proposes new cluster-based key management mechanism, which is based on hash mechanism. The proposed key management mechanism uses random key pre-distribution and multi-hop mechanism. The work considers that each node has their own pre-establish key and node will establish pairwise key with its one-hop neighbor, and with its multi-hop destination. The work considers the establishment of secure-link in between the one-hop neighbors and multi-hop destination node. Here, every node uses a simple-one way hash function to establish the keys in between one-hop neighbor and multi-hop destination.

The performance evaluation of work shows the comparative analysis in between attack situation, one-hop key management solution, and combined solution (one-hop plus multi-hop solution). The work is evaluated by considering three performance measures, packet loss rate, energy consumption, and delay. The evaluation also considers the effect of increasing malicious nodes on the performance of key management algorithm. The performance analysis shows that the one-hop solution shows improved performance in presence of an attack but the performance is further improved in larger extent by establishing secure-link for one-hop and multi-hop communication.

The remainder of the paper is organized in five sections. Section 2 describes the related work in hash-based key management algorithms with their advantages and disadvantages. It also derives the common disadvantages to be addressed in future work. Section 3 gives detailed insights into proposed hash-based key management mechanisms with considered system model, key establishment mechanism, and procedure to detect the malicious node in network. Section 4 discusses the simulation of the proposed mechanism with attack performance under one-hop solution and performance comparison of one-hop and one-hop plus multi-hop solution. Section 5 concludes the work with future work.

2 Related Work

The related work discusses recent key management mechanism based on hash key mechanism. Biming Tian et al. [6] describes a key management scheme for heterogeneous sensor networks which uses keyed-hash chain. It uses cluster-based approach to enhance the probability of key sharing between sensors and their cluster heads. It helps to improve the performance against node capture attack. The work proposes the establishment and renewal of five different types of keys in a network. The work shows promising probability of key sharing, but increases the computational overheads significantly, by introducing establishments and renewal of five different keys.

Walid Bechkit et al. [7] proposes an efficient and highly resilient key management scheme for WSN. It is based on symmetric cryptography with a probabilistic key pre-distribution. It uses simple hash function mechanism to enhance the resiliency of key management mechanism. The mechanism is highly resilient against node capture.

Rui Zhou and Hua Yang et al. [8] proposed a hybrid key management scheme for heterogeneous WSN based on Elliptic Curve Cryptography (ECC) and trivariate symmetric polynomial. Symmetric keys are used to establish the secure-link with the neighboring nodes. It uses a one-way hash chain to generate pairwise key with its neighbors. The dynamic key update mechanism is based on one-way hash chain and time slice mechanism. The proposed mechanism shows significant security enhancements and reduces the communication and storage overheads.

Qin Ronghua et al. [9] proposes a key management scheme for manually deployed wireless sensor networks based on dual directional hash chains. The work considers the honeycomb-like network arrangement for key management. The dual directional hash chain mechanism establishes the forward- and backward-hash chain to guarantee the forward- and backward-secrecy. Here, every node establishes the dual directional hash chain with other nodes in network. The work shows good security performance but it increases the network overheads and iss difficult to apply in real scenarios.

Baojiang Cui et al. [10] describes UBKM, a usage-based key management protocol for distributed sensor networks. It is based on four keys, which are derived from an initial master key. The mechanism uses hash-based authentication mechanism. The work shows significant security enhancements but increases the computational overheads of the system.

Table 1 surveys the hash-based key management solutions for secure communication between source and destination. The techniques focus on how the source will generate pairwise keys with its one hop neighbors. But for multihop secure communication, every in between node is supposed to establish pairwise key for the secure path communication.

Table 1 shows the comparative chart of the related work which highlights the different ways of applying hash-based mechanism for improving the

Table 1 Comparison of related work

Reference	Mechanism Used	Secure-Link Establishment	Advantages	Disadvantages
[6]	Key-hash chain	One-hop	Improved performance against node capture attack, Good probability of key sharing.	Increase energy and delay overheads because of establishment and renewal of five different keys.

Table 1 Continued

[7]	Probabilistic key Pre-distribution	One-hop	Improve Resiliency of key Management Mechanism.	Based on Symmetric Cryptography.
[8]	One way hash chain with ECC and trivariate symmetric polynomial	One-hop	Enhance the security using ECC and trivariate polynomial, Reduce the communication and storage overheads.	Not checked for energy, delay performance, the result shown does not prove the efficiency of mechanism.
[9]	Dual direction hash chain in honeycomb network	One-hop	Enhance security by guaranteeing the forward- and backward-secrecy.	Increase network overheads and difficult to apply in real scenario.
[10]	Usage based key management	One-hop	Improve security by using four different keys.	Increase the computational overhead.

security of WSN. The table lists the mechanisms used and its advantages and disadvantages. The major disadvantages of the work done are: they are not adaptable and scalable for changes in a network, limited to establishing secure link with single hop neighbors and not evaluated according to their effect on actual performance of WSN and effect of attack.

3 Proposed Hash Key-Based Key Management Mechanism

3.1 System Model

Figure 1 shows the considered system model for designing efficient key management schemes for a wireless sensor network. The system model shows the network which is divided into a number of clusters. The cluster is used to improve the scalability and energy efficiency of the system. Each cluster consists of a cluster head (CH) which aggregates the information from all sensor nodes (SN) in the cluster and transfers the aggregated information to the other CH or to the BS. The communication in between the SN to SN is intra-cluster communication, which takes place via SN to SN link. The transmission in between the CH to CH or CH to BS is inter-cluster communication, which takes place via CH to CH link or CH to BS link.

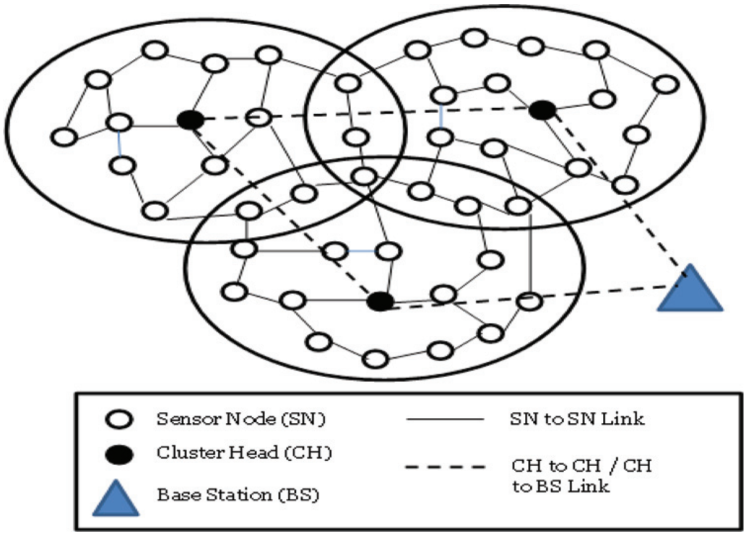

Figure 1 System model.

3.2 Key Establishment

The design of key management mechanism is based on random key predistribution and multi-hop mechanism. The work considers that the network is safe and reliable when the nodes are deployed in the initial stage. The work proposes that each sensor node will establish pairwise keys with its one-hop neighbor and its multi-hop destination node. Consider that each node is predistributed with an initial key K_i during node deployment. Each node N_x will use K_i and one-way hash function f to generate its master key $K_x = fK_i(ID_x)$. After the establishment of master key node N_x broadcasts an advertisement message $(ID_x, Nonce_x)$ that contains a nonce, and waits for each neighbour N_y to respond with its identity and then N_y responds with $(ID_y, (K_y, (ID_y | Nonce_x)))$. All messages are transmitted in an encrypted format inside the network. At the same time N_y will also generate the key $K_y = fK_i(ID_y)$ and both N_x and N_y will generate the pairwise key $K_{x,y} = fK_x(ID_y)$. After establishing pairwise keys with neighbouring nodes, the source node will establish the pairwise key with its multi-hop destination. Consider, N_x is the source node and N_n is the destination node. Hence, the pairwise key will be calculated as $K_{x,y,z,..,n} = fK_xK_yK_z \ldots, K_{n-1}(ID_n)$. The key establishment procedure for one-hop neighbor is as shown in Figure 2, the same procedure will be repeated for multi-hop neighbors.

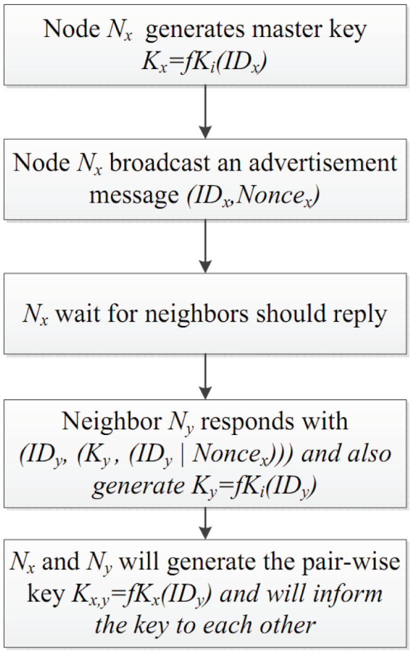
Node N_x generates master key K_x=$fK_i(ID_x)$
Node N_x broadcast an advertisement message $(ID_x$,$Nonce_x)$
N_x wait for neighbors should reply
Neighbor N_y responds with $(ID_y$, $(K_y$, $(ID_y \mid Nonce_x)))$ and also generate K_y=$fK_i(ID_y)$
N_x and N_y will generate the pair-wise key $K_{x,y}$=$fK_x(ID_y)$ and will inform the key to each other

Figure 2 Key establishment.

3.3 One-Way Hash Mechanism for Detecting Malicious Node

The hash function $F(p)$ is a transformation that takes an input and returns a one-way hash chain. The most important property of a one-way hash function [11] is that it has no inverse function $p = F^{-1}(q)$, which means for a given q, it is easy to compute $q = F(p)$; however, given F and q, it cannot determine p. Therefore, even if the adversary got the hash value q and the function F, they still have no ability to calculate the input value p.

During the initial stages, each node is pre-distributed: a pairwise keys initially with its neighbours and then with its multi-hop destination. The pairwise key K_i is used as a seed and associated with hash function $K_i = F(K_{i+1})$, $0 \leq i \leq n$ to generate an one-way hash function. When the member node N_x sends a packet to his CH, it includes a calculated hash number K_1 in the first packet, K_2 in the second packet and so on. CH use the pairwise key shared with the node Nx by hash function to generate the first hash number K_0. To validate the one-way hash function number, each CH maintains a verifier V_s for each member node N_x, initially, V_s is K_0. When N_x sends the n-th packet containing K_n to CH, the CH receives this packet and verifies via $V_s = F(K_n)$.

Having validated the packet correctly, the CH sets V_s to K_n. Generally, the CH can utilize the verification test iteratively up to a fixed number *IN* times, as $V_s = F(F... (F(K_{IN})))$. If the packet is not validated after *IN* times, the CH simply drops the packet, and the node N_x is considered a malicious node. Then the CH stores the malicious node's ID and announces the ID to all member nodes to exclude the malicious node. The same verification process is repeated on each hop and the final verification is done by using V_n verifier, if it is the *n*-th node in the network.

4 Simulation Results and Analysis

4.1 Simulation Details

The implementation is performed by using discrete event simulator NS-2 (Network Simulator-2). The parameters set during simulations are shown in Table 2. The idle power, receiving power, transmission power, and sleep power are considered according to IEEE 802.15.4 radio model [12]. The simulation considers 100 numbers of nodes arranged in the random number in 100 m × 100 m area. For doing this simulation we made the changes inside the node class of NS-2. NS2 is a standardized open source simulator which

Table 2 Simulation and node parameters

Parameter Name	Setting Used
Network Interface type	Wireless Physical:802.15.4
Radio Propagation Model	Two-Ray Ground
Antenna	Omni-directional antenna
Channel Type	Wireless Channel
Link Layer	Link Layer (LL)
Interface Queue	Priority Queue
Buffer size of IFq	50
MAC	802.15.4
Routing Protocol	Ad-hoc routing
Energy Model	EnergyModel
Initial Energy (initialEnergy_)	100J
Idle Power (idlePower_)	31mW
Receiving Power (rxPower_)	35mW
Transmission Power (txPower_)	31mW
Sleep Power (sleepPower_)	15μW
Number of nodes	100
Node Placement	Random
Number of simulation runs	20

considers the layered architecture of the network. For calibrating the results we have taken 20 runs of simulations. Final results are calculated by taking the average of 20 simulations runs. The simulation considers the malicious nodes, which attack by using a jamming attack. The implementation of jamming attack is performed by using discrete event simulator NS-2 (Network Simulator-2) by extending the node class. The implementation considers that the malicious nodes jam the network by repeatedly sending the malicious packet with random packet id and this repetition of packets leads to a collision in the network. The parameters set during simulations are shown in Table 2. The idle power, receiving power, transmission power, and sleep power are considered according to IEEE 802.15.4 radio model [12].

4.2 Simulation Results

4.2.1 Attack performance under one-hop solution

Figures 3, 4 and 5 shows the measurements of packet loss rate, energy consumption, and delay by varying the number of attacker nodes in the network. All these three results show that the performance of attack degrades after applying the one-hop key management solution. The attack situation increases the amount of packet loss in the network, which leads to an increase

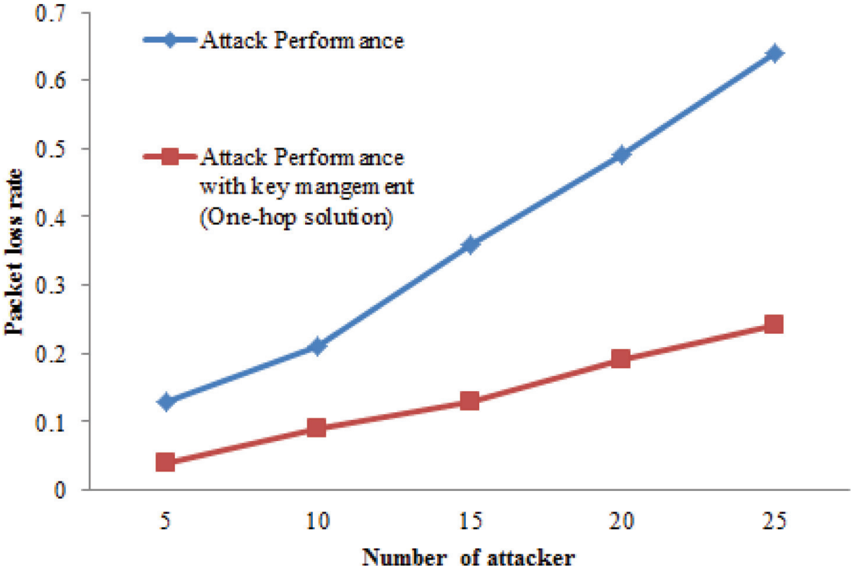

Figure 3 Measurements of packet loss rate by varying the number of attacker nodes.

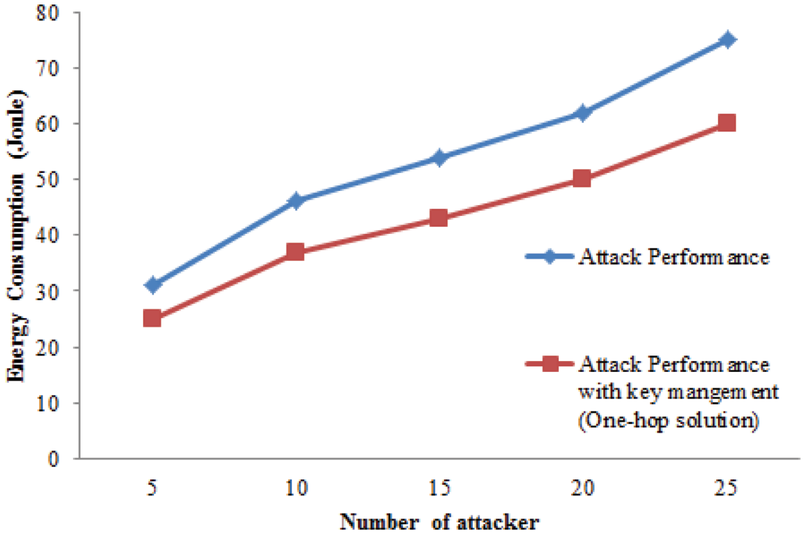

Figure 4 Measurements of energy consumption by varying the number of attacker nodes.

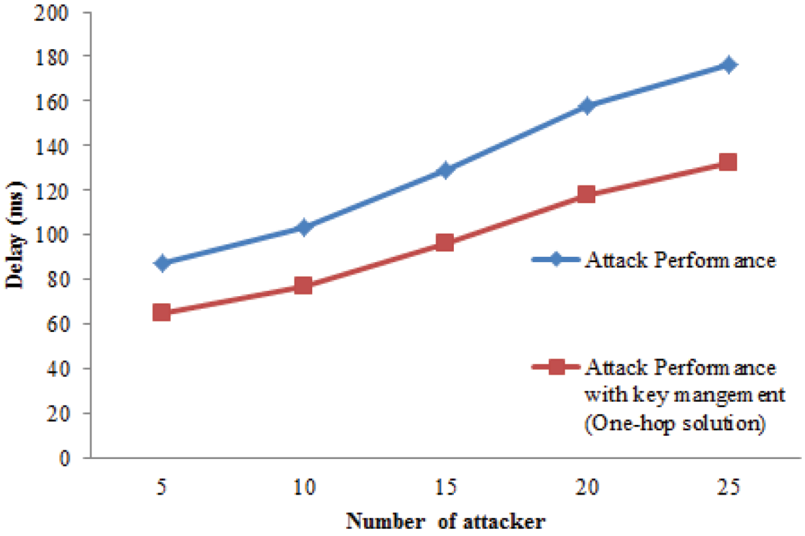

Figure 5 Measurements of delay by varying the number of attacker nodes.

in resend. The increase in resend of packets increases energy consumption of sensor nodes and also increases the amount of delay in the network. In opposite to this, other considered case reduces the packet loss rate with reduction in energy consumption and delay. Here, the network will detect a malicious node if the key validation process fails at CH sides and the CH repeatedly drops the packets. The key validation process checks each packet for the included key and applies the verification process. The verification process is performed by using a verifier function. If the function fails iteratively for a considered number of fixed time, the packet will drop. Henceforth, the network stops the communication via malicious node by removing the malicious node from the network.

4.2.2 Performance comparison of one-hop and one-hop plus multi-hop solution

Figure 6, 7 and 8 shows the performance comparison of one-hop solution and one-hop plus multi-hop solution by measuring packet loss rate, energy consumption, and delay with a varying number of attackers inside the network. The results show improvement in packet loss rate and energy consumption in case of combined solution (one-hop plus multi-hop). The reason of improved packet loss rate and energy consumption with combined key management solution is, the use of one-hop keys for neighbor communication and multi-hop key for communication with the final destination. In the case

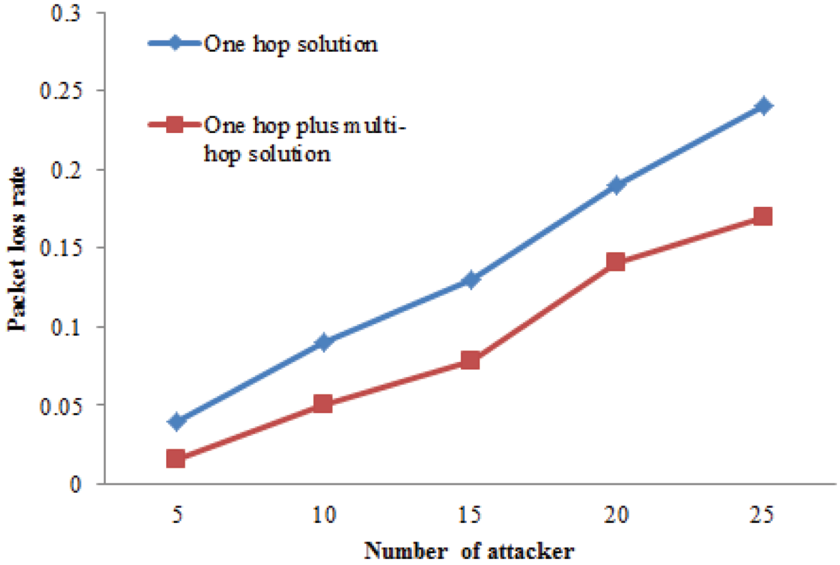

Figure 6 Comparitive packet loss rate performance of one-hop solution and one-hop plus multi-hop solution.

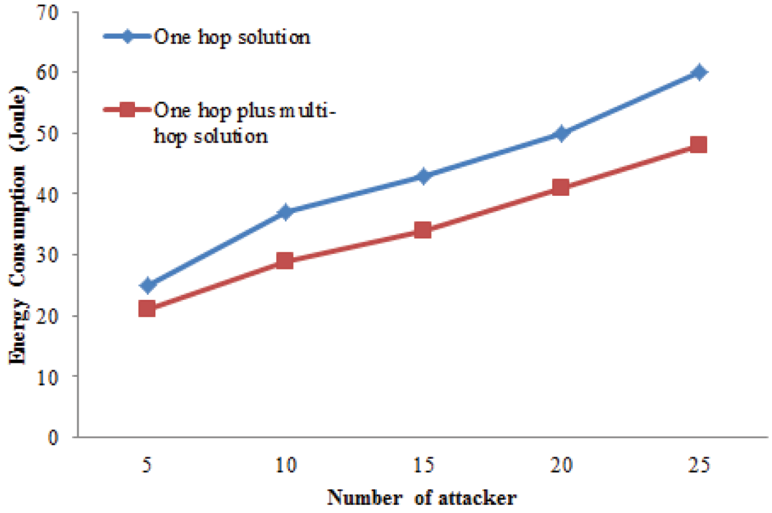

Figure 7 Comparitive energy consumption performance of one-hop solution and one-hop plus multi-hop solution.

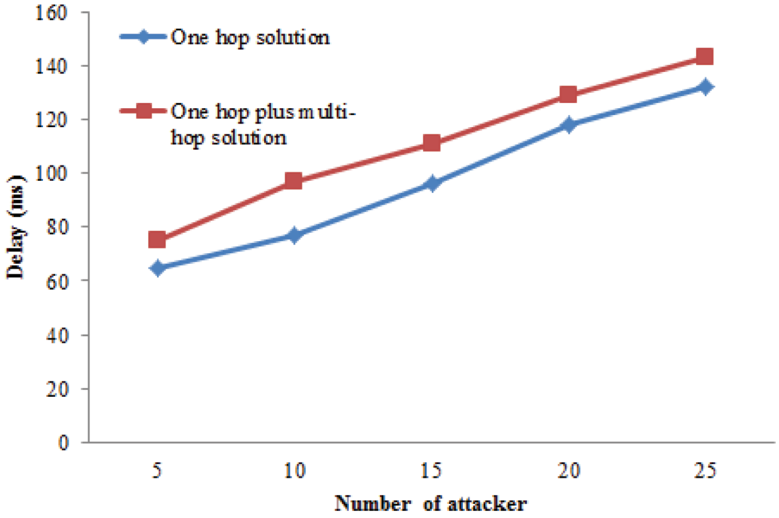

Figure 8 Comparitive delay performance of one-hop solution and one-hop plus multi-hop solution.

of a combined solution, the verification process has two levels: one is on hop-to-hop basis and the second level verification is at final multi-hop destination.

The result shows the tradeoff of delay for improving the packet loss rate and energy consumption. The key establishment and verification process, at one-hop and multi-hop level leads to increase in delay.

In network there two types of communication: one is hop to hop communication which works at data link layer and the other is source to destination i.e., multihop which work at network layer. So our alogrithm tries to give security at both layers. The paper uses simple one-way hash function so that the overheads of key establishment and key exchange are reduced a lot. The Verifier function also takes care of whether the hash key is generated properly or not in the entire communication path.

5 Conclusions and Future Work

The importance and need of security solution is increasing in WSN as the number of attack situations are increasing in WSN. The key management solutions are playing a major role in saving WSN from different attacks such as a jamming attack. The paper surveys recent hash-key based key management mechanisms and proposes the new hash-key based key management solution for cluster-based WSN. The proposed key management solution does the key establishment and verification process at two levels (First at one-hop and second at multi-hop destination). If attacks happen on security solutions, then first the proposed security solutions will detect the attacker node and then it will mitigate the attack by removing attacker node out of the network. The mechanism shows good energy efficiency and reduced packet loss rate as compared with hash-key based one-hop solutions.

In the future, the work can be extended to find the more efficient solution by considering the mobile WSN.

References

[1] Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., and Galloway, M. (2007). A survey of key management schemes in wireless sensor networks. *Comput. Commun*. 30, 2314–2341.

[2] Zhang, J., and Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. *J. Netw. Comput. Appl.* 33, 63–75.

[3] Babar, S. D., Prasad, N. R., and Prasad, R. (2013). Activity modelling and countermeasures on jamming attack. *J. Cyber Secur. Mobil*. 2, 1–22.

[4] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Commun. Surv. Tut.* 11, 42–56.

[5] Raymond, D. R. and Midkiff, S. F. (2008). "Denial-of-service in wireless sensor networks: attacks and defences." *IEEE Pervasive Comput.* 7, 74–81.

[6] Tianm, B., Han, S., and Dillon, T. (2009). "A key management scheme for heterogeneous sensor networks using Keyed-Hash chain," in *Proceedings of the Mobile Ad-hoc and Sensor Networks '09*, Fujian, 448–456.

[7] Bechkit, W., Challal, Y., Bouabdallah, A., and Bencheikh A. (2010). "An efficient and highly resilient key management scheme for wireless sensor networks," in *Proceedings of the 35th IEEE LCN*, Denver, CO, 216–219.

[8] Zhou, R., and Yang, H. (2011). "A hybrid key management scheme for heterogeneous wireless sensor networks based on ecc and trivariate symmetric polynomial," in *Proceedings of the IEEE URKE*, Bali, 251–255.

[9] Ronghua, Q., Qi, S., Xing, Y., and Xiaobing, Y. (2012). "A key management scheme for manually deployed wireless sensor networks based on dual directional hash chains," in *Proceedings of the IEEE ISDEA*, Sanya, 752–755.

[10] Cui, B., Wang, Z., Guo, T., Dong, G., and Zhao, B. (2013). "UBKM: A usage-based key management protocol for distributed sensor networks", in *Proceedings of the IEEE EIDWT*, Xi'an. 267–272.

[11] Hsieh, W.-B., and Leu, J.-S. (2013). "A dynamic identity user authentication scheme in wireless sensor networks", in *Proceedings IEEE IWCMC*, Sardinia, 1132–1137.

[12] Corbett, D. J., Ruzzelli, A. G., Everitt, D., and O'hare, G. (2006). *A Procedure for Benchmarking MAC Protocols used in Wireless Sensor Networks Technical Report 593*. Sydeney, NSM: University of Sydeney, 1–28.

Biographies

S. D. Babar is ISTE Life Member. He is awarded the Ph.D. Degree in Computer Engineering from Aalborg University, Denmark in the area of Wireless communication on 25th Feb 2015. He is graduated in Computer Engineering from Savitribai Phule Pune University, Maharashtra, India in 2002 and received Master in Computer Engineering from Savitribai Phule Pune University, Maharashtra, India in 2006. He is currently working as Professor and Head in the department of Computer Engineering, Sinhgad Institute of Technology, Lonavala, India. He has 15 years of teaching and research experience. He has published more than 30 papers at national and international level. He has authored two books on subjects like Software Engineering and Analysis of Algorithm & design. He has received the Cambridge International Certificate for Teachers and Trainers at Professional level under MISSION10X Program. He is IBM DB2 certified professional. His research interests are Data Structures, Algorithms, Theory of Computer Science, IoT and Security.

P. N. Mahalle has obtained his B.E. degree in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, India and M.E. degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. He completed his Ph.D. in Computer Science and Engineering specialization in Wireless Communication from Aalborg University, Aalborg, Denmark. He has more than 16 years of teaching and research experience. Currently he is working as Professor and Head in Department of Computer Engineering at STES's Smt. Kashibai Navale College of Engineering, Pune, India. He has published 61 research publications at national and international journals and conferences with 265 citations and H index 8. He has 5 Patents to his credit. He has authored 8 books at National and International level. He has guided more than 100 plus undergraduate students and 20 plus post-graduate students for projects. His recent research interests include Algorithms, Internet of Things, Identity Management and Security.