Domain unlimited false data filtering schemein wireless sensor networks

Jinguo Zhao[1*],Qingyun Luo[1],Xin Li[1],Junbin Liang[2]

[1]*School of Computer and Information Science, Hunan Institute of Technology,Hengyang*

[2]*School of Computer and Electronics Information, Guangxi University, Nanning*

Received 9October 2014, www.cmnt.lv

Abstract

The false data filtering scheme of WSN has no way to detect the false data injected from the non-forwarding area of the compromised nodes. For this, two schemes are proposed in the article. The first one is that false data are filtered by combining the information of the forwarding path with threshold method. Each forwarding sensor not only checks the correctness of the MAC carried in the report, but also validates two security threshold parameters. The second one does not utilize the information of transmission path, but filter false data in the course of transmission, based on the distribution of secret keys in the whole key pool. Theoretical analysis and simulation experiment show that both the two schemes can detect the false data injected from any area on the network, with low energy consumption and high security.

Keywords: wireless sensor network, false data filtering,MAC, key pool, threshold method

1 Introduction

Wireless Sensor Network (WSN) has a widespread application prospect in national defence and military, environmental monitoring, medical treatment and public health, and human body monitoring, so WSN is a very active field of research[1]. Sensor nodes are usually deployed in the severe surroundings, or even in the enemy areas. Cluster heads normally need multi-hop so that they can transmit the data to the base station, and nodes are easily trapped. Thus, an attacker, by using the secret key saved in the node, can fabricate a false event which did not really happen(such as tanks coming and going), and maliciously tamper with the teleporting data package and transmit repeated data packages and so on. With no precaution, false data will lead to false alarms, disturbing users of their decisions and expending the limited network resource. In addition, once a node is captured, an attacker can easily get and make use of the information of the secret key saved in the node to fabricate false data and transmit it to his neighbour node through the compromised node. This neighbour node will have difficulty making a judgment whether the data package is true or false. Consequently, it is a challenging problem how to identify and filter the false data in WSN[1-4].

Fortunately, some progress has been made about the research on the identification and filtration of false data in WSN[4-14]. Technically, these methods are mainly based on the idea of digital signature. *t*Message Authentication Codes(MAC) are added to the back of the data package which is to be transmitted, and the authentication of data package is completed in the course of the data transmission, which, thus, implements the identification and filtration of false data[4]. Here *t* is threshold value. The schemes can be employed to detect the false data packages injected from the transmission area of the compromised node. If an attacker, however, injects the false package from the non-forwarding area of the compromised node into the network, the intermediate node will have no way to detect and filter.

According to different ways of key distribution to the problems, the false data filtering mechanism in WSN can be divided into two types: the filtering mechanism of the key distribution based on the pre-deploy and the filtering mechanism of the key distribution based on the post-deploy.

The filtering mechanism of the key distribution based on the pre-deploy mainly has SEF[4] and FFRF[5].Ye et al have suggested SEF mechanism that a global key pool be fallen into multi-partitions of secret key and each node is preset partial key in a secret key partition by random selection. If any event happens, multi-nodes for detection are united to generate a data report including *t* MACs and guarantee the secret keys having generated MAC to come from different key partitions. If a secret key is the same as the detecting nodes at the stage of forwarding filtration, the intermediate node will regenerate a MAC with the key and verify the MACs carried in the data package. Finally, Sink has the information on the global secret key and is equipped with great powers to calculate, communicate and store; thus, all the false packages can be filtered. Yet, the key has not been bound with the surveyed area, once an attacker captures *t* different key

[*]***Corresponding author's*** e-mail:zhaojinguohit@163.com

partitions, he can be free to fabricate a false data package without being recognized by transfer nodes.

Zhou et al. came up with a filtering scheme, FFRF[5], based on Hash function. FFRF divided nodes into probe node and check node, and preloaded each node with identical one-way function, and thus generated a one-way Hash chain c_1, c_2,…,c_t. Every originating node made the original Hash value open. Forwarding node verified the correctness of Hash value by means of the pre-stored, verified Hash value. In addition, it validated MAC in data package with the shared symmetric key in order to filter the false data. Sink could filter the false data further by verifying Hash value again, and also it could roughly locate the compromised node through verifying the exclusive OR of each MAC. FFRF did not bind node key with Hash value; therefore, it is easy for an attacker to get legal Hash from legal package so as to break through the security mechanism.

Li et al proposed a filtering scheme, PVFS[6], based on cluster organization and voting mechanism. PVFS organized nodes to clusters. A shortest path was established from each cluster head to Sink.Forwarding nodes were all cluster heads. The key of a node in originating cluster was stored at the probability $d_i/d_0.d_0$and $d_i$were hop counts from originating cluster or forwarding cluster to Sink. Once an event happened, the sensor node brought out a Vote(The function of Vote is similar to MAC). Data report was just produced by the Votes which were generated when cluster head collected t nodes in cluster. Upon forwarding, the forward cluster head verified data at a certain probability. Yet, much bigger semi-diameter for communication was needed between cluster heads than common nodes in order to forward data, which caused cluster heads to run out of their energy very quickly.

The filtering mechanism based on the post- deploy key distribution mainly includes IHA[7]and GRSEF[8]. Zhu et al first brought up anintersectional and step-by-step authentication mechanism when routing.The post-deployed nodes formed clusters, and a path was established from every cluster head to Sink. In the path a cooperative relationship was set up between the nodes at a distance of t+1 hop counts. When an event took place, every sensor node, through the private key sharing with Sink and the pair-wise key sharing with the downstream cooperative nodes, respectively engendered 2 MACs. Cluster head collected MACs of t+1 sensor nodes to generate data report.Upon forwarding, each node checked and corrected MAC brought by the upstream cooperative nodes.After successful verification, a new MAC formed and replaced the verified MAC by means of the key sharing with the downstream cooperative nodes. IHA could filter the false package in t hop counts, but its way of key distribution was not suitable to dynamic WSN route, which required a large number of expenses for maintenance.

Yu et al. put forward a false data filtering scheme based on multi- coordinate axis. Before deployment, each node was preloaded with parameters such as network topology and a key shared with Sink. After deployment, the nodes were just divided into t groups, which ensured that each location was just covered by t key partitions. Then based on multi-axis, the same keys were distributed to the nodes of the same group. During forwarding, the intermediate node checked and corrected MAC in the data package by utilizing the pre-shared keys. Finally, all the false packages that missed forward and filter were filtered by Sink. GRSEF could accommodate multi-Sinks and dynamic Sink, but it required every node equipped with the expensive positioning device like GPS. So its expenditure was too much.

SEF, FFRF, IHA and GRSEF could not filter the false data immitted from the non-forward zone of the compromised node. This article mainly studied false data filtering strategies.

2 Basic framework of forwarding filtration

The basic framework of forwarding filtration mentioned in Reference[4]includes four sections: key distribution management, data report generating, forwarding filtration and Sink checking.Key distribution management is to establish key correlation between nodes and form key-sharing relation. The management is the core of filtering mechanism. The capability of forwarding filtration depends on the key-sharing degree between nodes, so the increase of key-sharing degree will lead to the improved power of forwarding filtration and much information on the key stored by each node. Therefore, key distribution mechanism should ensure the secret keys while

Data report generating is that when any event takes place, each sensor node(origin node), with the stored key, encrypts data and obtain MAC (Message Authentication Code); then, multiply sensor nodes, by using MAC and their corresponding key index, jointly generate data report. A legal data report must carry t MACs from different detecting nodes.

Forwarding filtration is first to examine whether a data package attaches t MACs from different detecting nodes when nodes receive the data package，and then regenerate a MAC with the stored key corresponding to the data package and compare whether it is the same as the MAC to be checked in the data package. If the detection at any step is not passed, the data package is abandoned right away. If nodes do not store the corresponding secret key, the data package is directly forwarded.

Forwarding filtration is a kind of probabilistic filtration which has no way to detect all the false data packages and abandon them, so Sink node is used as the last par close to identify and abandon all the false data that arrive at last. Sink possesses global key information, adequate energy and great computing power so much that it can check all the MACs in a package. If all the MACs are checked to be correct, Sink will receive a data package; otherwise it will abandon the data package.

3 The filtering scheme based on Threshold mechanism

3.1 SYSTEM MODELS AND RELEVANT ASSUMPTIONS

Assume that each sensor node should have the onlyID and be safe in the short period of time after distributed. After deployment, clusters are organized by means of the mechanism of clusters. Assume that the density of distribution of the sensor node be big, and at least t nodes be sensed in the same cluster after event occurrence. Each sensor node generates MAC after the event is encrypted by using secret key, and then MAC and positional information are sent to the cluster head so as to generate data reports.

General sensor nodes with weaker capacity are easily captured, while Sink node unable to be compromised can sense and filter the false package which finally reached, equipped with adequate energy, powerful compute and communication capacities, and global secret information. After capturing nodes, attackers can counterfeit false data package and sent it to the Internet by taking advantage of the secret information stored in nodes, or falsify the legal data package in transmitting by using compromised nodes[3]. And this article develops a solution only to the attack of the injected false data.

3.2 DATA REPORT GENERATION

After sensing an emergency, the cluster head CH_icollects the perception data of the nodes in the cluster and selects a relatively complete value e as the description of this emergency, and then broadcasts it in the cluster. The node $S_i$in the cluster compares e with the data sensed by itself. If the deviation is in the range of an allowed threshold value, the perception data are encrypted by using the master cryptography key$K_i$sharing with Sink so that M_i:K_i(e) is generated. Afterwards, in thepairwisekeyschemeS_i encrypts the signature and send it to the cluster head CH_i, which collects the signatures of t different nodes and forms the data package R. Equally in the pairwise key scheme the data package isencrypted and then sent to the next hop cluster head.

3.3 FORWARDING FILTRATION STAGE

First, the value-calculation procedures of the two parameters $T_{v\text{-}max}$ and $T_{c\text{-}max}$ are given, and then the process of transfer filtration is introduced. t MACs are attached to every data package, which means all the t MACs has successfully been validated. So the follow-up nodes don't have to validate the data package. If there are N_c compromised nodes in the network, the attacker would surely fabricate(t-N_c) false MACs in order to concoct a false data package. If the probability of one filtered hop, transmitted by the false package in the forward path of the compromised node, is p_a, the number of the hops transmitted by it in the path is about

$$\sum_{i=1}^{\infty} i \times (1-P_\alpha)^{i-1} \times P_\alpha = \frac{1}{P_\alpha}. \quad (1)$$

If $T_{c\text{-}max}$=1/p_a, $T_c > T_{c\text{-}max}$, which means 1/p_a hop, continuously transmitted by the data package in the forward path, is not validated. So the data package is the false data package immited by the attacker from the non-forward zone of the compromised node.

When a relay node receives data package, R is validated as the following steps:

1) First, check whether the statusidentifier*flag* of the data package is 1. If so, it means all MACs has been validated successfully, and there is no need to validate the data package. Thus the relay node just forwards data package.

2) If *flag* is not 1, check whether the number of MAC in the data package is t. If it is more or less than t MACs, the data package R can be discarded right away.

3) If the number of MAC meets the demand, retrieve the key index table. If the same key as the one in the data package R is not stored, T_c should be added 1. Next, is (T_c=$T_{c\text{-}max}$) true? If it is true, it means R has had continuous transmission of $T_{c\text{-}max}$hops but not validated them. We have concluded that the data package is the false one injected by the attacker from the non-forward zone of the compromised node. So R can be immediately discarded, and the verification process is over. If (T_c=$T_{c\text{-}max}$) is false, data package can be transmitted.

4) If relaying node has the same key as the one in the data package$R$, another MAC is recalculated with the key and e. If the two MACs are equal, that means the success of verification. Make T_c is 0, T_v plus 1, and the zone bit corresponding to the MAC in Bin_v is 1. Next, judge whether (T_c=$T_{c\text{-}max}$) is true or not. If it is true, make *flag* =1, finish the verification process, and forward data package; if it is false, forward data package. If the calculated MAC is not equal to the verifying MAC, it means the failure of verification. Discard data package.

3.4 SINK FILTRATION

Sink node has global key information and the positional information of all the nodes, with so powerful calculation and storage capacities, and so adequate energy that all the false data can be filtered even if they have skipped transfer validation. When Sink receives data package, all MAC and the positional information of sensor nodes are validated again. If they are all true, accept data package and execute relevant decisions; otherwise, discard data package.

4 Filtering scheme of key distribution based on pre-deploy

After deploy, the problems about distributing keys are as follows:

1) On the course of establishing the relation of sharing keys after node deploy, symmetric keymechanism and session keymechanism in which much expense would have to be spent on communication must be adopted so as to avoid pure key being directly transmitted in the communication link. Therefore, the cost is too much.

2) Once the cluster head is captured on the course of key distribution, the key it blabs will cause the security mechanism invalid. So it is not secure.

3) After deploy, key distribution will take a long time to astringe, and network fails to carry through in-situ monitoring and data sense. Before deploy, PKFS distributes keys and then the forward node filters false package at a certain probability.

4.1 KEY DISTRIBUTION

Each sensor node is given a unique *ID* before deploy. Suppose the node number in the network is *N* and the key sharing degree expected to realize is *n*/*N*in the practical application, establish a global key pool

$$G = \{K_i : 0 \le i \le m-1\} . \quad (2)$$

as big as *m*, *m* = *N*/*n*. Next, divide network nodes into m groups which are respectively marked as $g_1,...,g_m$. Group *i* is

$$g_i = \{S_1, S_{m+i},..., S_{L(g_i)*m+i}\}, L(g_i) = g_i . \quad (3)$$

4.2 DATA REPORT GENERATION

After key distribution is finished, nodes are well-dispensed at random. When an event occurs, it is sensed at the same time that multiple nodes of the sudden event jointly generate a relatively complete value *e* as the description of the event, and a center node CoS is selected. After that, every sensor node encrypts *e* with keys to create M_i:$K_i(e)$, and the node number and MAC are sent to the center node, which selects out *t* MACs caused by the nodes from different groups(included the center node itself), and data package *R* forms.

4.3 FORWARD FILTRATION

Part of keys in the key zone, the geographic positions of part of nodes, and key zone index are pre-loaded at random, so the intermediate node can validate MAC, node position and key index in data package at a certain probability.

When receiving the forwarded data package *R*, the intermediate node carries through the following steps for validation:

1) First, check whether the number of MAC in data package is *t*. If it is more or less than *t*, just discard the data package.

2) Secondly, if the number of MAC meets the demand, check whether *t* node numbers in data package is from different groups. For example, (N_i-N_j) mod *m*=0, it means N_i and N_j are from the same group. If any two nodes in data package are from the same group, discard the data package.

3) Then, if *t* nodes are from different groups, retrieve the key index table. If the same key is not stored as the one in the data package *R*, forward the data package. Otherwise, recalculate a MAC by using the stored key and *e*, and compare it with the to-be-validated MAC. If the two MACs are equal, it means a successful validation. If they are not so, discard the data package.

Finally, *if* the above validations are passed, forward R to the next hop node.

5 Property analysis and simulation result

5.1 SECURITY ANALYSIS

TMFS conducts the key distribution in a short period of time after node deploy. If in the short period of time any node is compromised, attackers can take advantage of the compromised node to interfere with key distribution, even make key divulged, which affects the whole property of the filtering mechanism Besides, as the existing mechanisms, if attackers inject false data from the forward zone of compromised node, the upstream node can use the sharing key to filter the false data quickly. On the other hand, if attackers inject false data from the non-forward zone of compromised node, when the hop number that false data have transmitted is over the threshold value$T_{c\text{-}max}$, the false data will also be filtered. Therefore, with key authentication mechanism and threshold exceeding mechanism, TMFS can filter the false data injected from any zone in the network.

Based on the key connectivity expected in the practical application, PKFS divides nodes into groups to construct the global key pool, and then distributes keys before node deploy. This key distribution has three characteristics: first, compared with the distributed keys after deploy, the way of distributing keys before deploy can be used to eliminate potential safety hazards; secondly, Dual key management mechanism must be employed in key distribution after deploy so as to ensure the safety of key transport,while by distributing keys before deploy, pure key can be directly transmitted to the corresponding node, which costs low energy. Finally, based on global nodes distributing keys, the false data package injected from any zones in the network can be filtered at the same probability.

5.2 FILTRATION EFFICIENCY

If N_c nodes in the network are compromised, attackers need to counterfeit(*t*-N_c) false MACs in order to fabricate a false data package. We make a comparative analysis in

PVFS mechanism, and the probability of one transmitted hop filtered in PVFS is p_v.

In TMFS, the false packages injected by attackers from the non-forward zones of compromised nodes are transmitted at most t hops in the network. So the probability of one transmitted hop filtered is $1/t$. And in the network the probability of one filtered hop transmitted by a false package that an attacker injects from the forward zone of the compromised node is p_v. When attackers inject false packages from the forward and non-forward zones of the compromised node in the proportion of $1/\alpha$,the probability of one filtered hop transmitted by a false package in the network is

$$P_{tm\_1} = \frac{1}{\alpha+1} \times P_v + \frac{\alpha}{\alpha+1} \times \frac{1}{t} \tag{4}$$

and the probability of h filtered hops transmitted by it is

$$P_{tm\_h} = 1 - (1 - P_{tm\_1})^h . \tag{5}$$

In PKFS, the probability of one filtered hop transmitted by a false package that an attacker injects from any zone in the network is

$$P_{pk\_1} = \frac{t - N_c}{m} \tag{6}$$

and the probability of h filtered hops transmitted by it is

$$P_{pk\_h} = 1 - (1 - P_{pk\_1})^h \tag{7}$$

Figure1 shows the comparison about the probabilities of filtration in TMFS, PKFS and PVFS[3]. Attackers inject false packages from the forward and non-forward zones of the compromised nodes in the proportion of 1/1; N_c=2; m=17; N=340. From Figure 1, it can be seen that when attackers inject false data from any zone, both TMFS and PKFS can filter false data at higher probabilities than the probability in PVFS which is lower for filtering false data. For example, when H=10, TMFS, PKFS and PVFS filter false data respectively at the probabilities 97.3%, 95.6% and 21.4%. Due to the verification of MAC in the data report that PVFS makes by means of intermediate node, only the false data injected from the forward zone of compromised node can be filtered;TMFS and PKFS, however, through intermediate node, verify the validity of originating node which generates data, so they can filter false packages injected from the forward and non-forward zones of the compromised node at the same time.

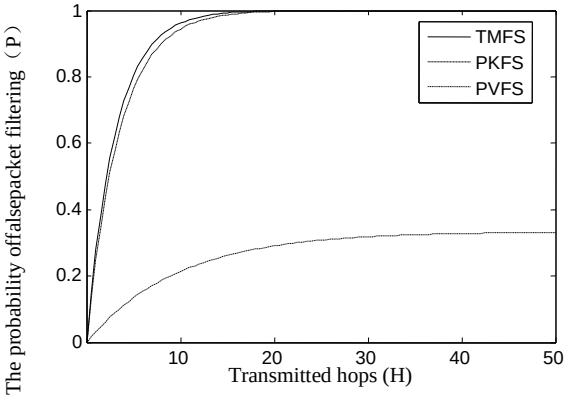

FIGURE1 Changes of the probability(P) that false packages are discarded with transmitted hops (H)

5.3 ENERGY CONSUMPTION

Reference 12 indicates that compared with the energy with which data packages are transmitted, the consumption can be ignored. So we just consider the energy consumption of data forward. Compared with the filtering mechanism in existence, TMFS adds 3 zone bits and a character string to data package, and the length of data package in PKFS are equal to the one in SEF.

In the same way as SEF[4] and PVFS[6], we employ the following model to make quantitative analysis of energy consumption. Suppose I_r, I_n, I_M, I_f and I_b respectively are the lengths of plain data package, node number, MAC, zone bit and character string without security mechanism, In TMFS, the length of data package

$$I_{r_{tm}} = I_y + (I_m + I_n) \times t + 3I_f + I_b \tag{8}$$

in PKFS, the length of data package

$$I_{r_{pk}} = I_y + (I_m + I_n) \times t \tag{9}$$

Suppose that the energy(E) is consumed when 1 rightful datum and a false data are transmitted, and that transmission distance is H (hop), the energy consumptions E_{tm} and $E_{pk}$of TMFS and PKFS can be showed as followed:

$$E_{tm} = \left[1 + \frac{I_m + I_n}{I_r} \cdot t + 3I_f + I_b\right] \cdot \left[H + \beta(H - \sum_{i=1}^{H-1} P_{tm})\right] \tag{10}$$

$$E_{pk} = \left[1 + \frac{I_m + I_n}{I_r} \cdot t\right] \cdot \left[H + \beta(H - \sum_{i=1}^{H-1} P_{pk\_i})\right] \tag{11}$$

Figure2 shows the comparison of energy consumption when 100 false packages transmit 20 hops respectively in TMFS, PKFS and PVFS, among which the number of the compromised node that an attacker captures (N_c) is 4, and

other parameter values respectively are: I_r ＝24bytes; I_n=10bits; I_M=64bits; N=1000.From Figure2, it can be seen that in PVFS the energy consumption of data package transmitting is rapidly on the rise with the increasing of false data number (β) and the number of MAC (t) carried by each data package. For example, when β=0 and t=5, the energy consumption in PVFS is only 120. But when β=10 and t=9, the energy consumption in PVFS goes up to 845. InTMFS and PKFS, the energy consumption of data package transmitting is slowly on the rise with the increasing of β and t. For example, when β=10 and t=9, the energy consumptions in TMFS and PKFS are 170 and 190 respectively. So compared with PVFS, the advantages of TMFS and PKFS can be obviously seen in saving energy.

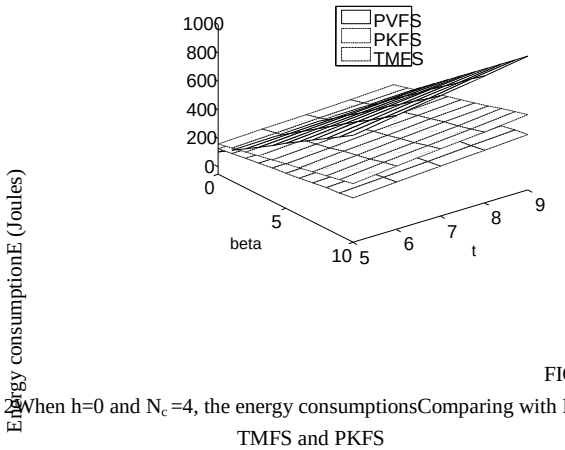

FIGURE 2 When h=0 and N_c =4, the energy consumptionsComparing with PKFS, TMFS and PKFS

5.4 SIMULATION EXPERIMENT

In order to verify the properties of TMFS and PKFS further, C++ language was used in this article to establish an analog simulation platform. In the experiment, the sizes of data packages adopted in TMFS, PKFS and SEF were 72bytes, 70bytes and 70bytes respectively; the power dissipations with which nodes sent and received a data package of 72bytes were 6.2×10^{-3}J(Joule) and 1.25×10^{-3}J respectively, and the power dissipations with which nodes sent and received a data package of 70bytes were 6×10^{-3}J and 1.2×10^{-3}J[3].Simulation setting was as followed: in a round network area of $\pi\times45\times45m^2$, a static originating node and a static Sink were respectively on the center of the circle and on the circumference, and the other 340 nodes were distributed at random. The originating node generated a false data package every 2 seconds, which amounted to 100 data packages. Perceived radius and communication radius of nodes were 5m and 2.5m respectively. Due to space limitations, only the experimental data about filtration probabilities and energy consumptions in TMFS, PKFS and PVFS were given. The average value of 10 simulation experiments was taken as the experimental result.

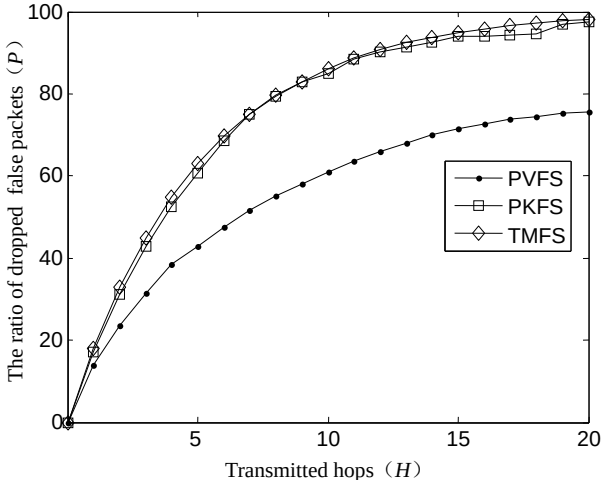

FIGURE 3 Filtration probabilities

Figure3 shows the changes of filtration probability(P) with transmitted hops(H), and the false packages injected from forward and non-forward zones of compromised nodes were both 50. From Figure3, it could be seen:

1) The more hops false package transmitted in the network, the higher the probability of its filtration was. For example, in TMFS, when H was 5 and 10, P was 60% and 85%;

2) The performance of TMFS and PKFS filtering false packages was far better than PVFS. For instance, when H was 15, the filtration probabilities of TMFS, PKFS and PVFS were 95%, 93% and 69%, respectively.

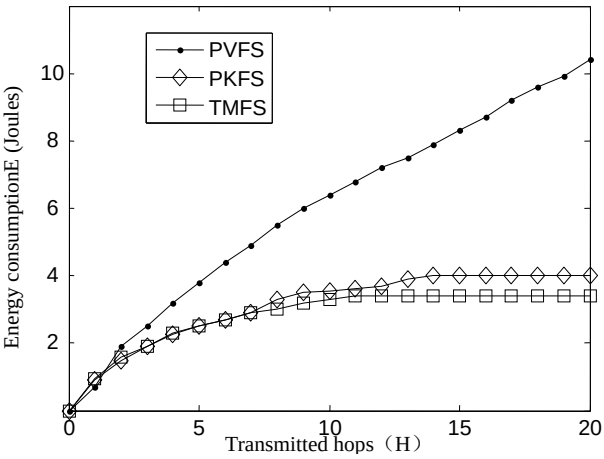

FIGURE 4 Energy consumption

Figure4 shows the comparison of energy consumption with which 100 false data packages caused by originating node were transmitted in TMFS, PKFS and SEF. From Figure4 it could be seen that the energy consumptions were far lower in TMFS and PKFS than in PVFS. For instance, when H is 10, the energy consumptions of false package transmission in TMFS, PKFS and PVFS were 3.6Joules, 3.7Joules and 6.5Joules. TMFS and PKFS could filter false packages injected from non-forward zone of compromised node as soon as possible, so they could save more energy than PVFS.

6 Conclusion

This article has covered two solutions to the problem that in the existing schemes false data injected from the non-forward zone of compromised node could not be detected and recognized in the sensor network.The first solution is TMFS based on threshold mechanism,in which nodes after deploy were established forwarding path to Sink; each data package involved *t* MACs of detecting node and 2 safety thresholds; forwarding node verified not only MAC, but also threshold value. In which a global key pool was constructed according to the expected keys-sharing degree, and each node was initialized a key before deployment. Analysis and simulation results demonstrated that both TMFS and PKFS could resist false data injection attacks from non-forwarding areas of compromised nodes, and consumed less energy than existing schemes.

Acknowledgments

Supported by the National Natural Science Foundation of China under Grant (No. 61379117,61173169);the Scientific Research Fund ofHu'nan Provincial Education Department of China under Grant (No.13C205,13C210).

References

[1] Ren F Y, Huang H N, Lin C 2003 Wireless sensor networks*Journalof Software***14**(7)1282-91

[2] Su Z, Lin C, Feng F J 2007 Key management schemes and protocolsfor wireless sensor networks*Journal of Software***18**(5)1218-31

[3] Liu Z X, Wang J X2012 Geographical information based false report filtering scheme in wireless sensor networks*Journal on Communications***33**(2)156-63

[4] Chong C, Kumar S 2003 Sensor networks: Evolution, opportunities, and challenges *Proeeedings of IEEE***91**(8)1247-56

[5] Ye F, Luo H, Zhang L 2004 Statistical en-route filtering of injected false data in sensor networks *Proceedings of 23th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM'04[C].Hong Kong China* 2446-57

[6] Zhou L, Ravishankar C 2005 A fault localized scheme for false report filtering in sensor networks *Proceedings of the IEEE International Conference on Pervasive Services (ICPS 2005)*59-68

[7] Li F, JW 2006 A probabilistic voting-based filtering scheme in wireless sensor networks *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC 2006)*255-65

[8] Zhu S, Setia S, Jajodia S 2004 An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks *Proceeding IEEE symposium on Security and privacy, S&P'04[C]. BerkleyCA USA* 259-71

[9] Yu L, Li JZ2009 Grouping-based resilient statistical en-route filtering for sensor networks *Proceedings of 28th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2009)* 1782-90

[10] Lu R, Lin X, Zhu H 2012 *Parallel and Distributed Systems, IEEE Transactions on***23**(1) 32-43

[11] Ayday E, Delgosha F,Fekri F 2007 Location-aware security services for wireless sensor networks using network coding*IEEE Conference on Computer Communications, INFOCOM'07[C]. Anchorage Alaska USA*1226-34

[12] Duda R O, Hart P E, Stork D G2012 Pattern classification*Hoboken: Wiley*

[13] Zhang S G, Zhou X H, Yang F, et al. 2014 A false report filtering scheme based on neighbor watch for wireless sensor networks*Journal of university of science and Technology of China***44**(4)317-24

[14] Bashir AK, Lim SJ, Hussain CS, Park MS*2011* Energy efficient in-network RFID data filtering scheme in wireless sensor networks*IEEE Sensors Journal* 7004-21

Authors

Zhao Jinguo, June1965,Shaodong county,Shaoyang city, P.R.China.

Current position, grades:associate professor level of School of computer and information science in Hunan institute of technology.
University studies:MSc of computer and communication engineering college of Hunan university.
Scientific interest:wireless sensor network.
Publications:10 papers.
Experience: teaching experience of 12 years,10 scientific research projects.

Luo Qingyun, October 1965,Shaodong county,Shaoyang city, P.R. China.

Current position, grades:professor level of School of computer and information science in Hunan institute of technology.
University studies: BSc from the school of information engineering of center south university.
Scientific interest: wireless sensor network
Publications:15 papers.
Experience: teaching experience of12 years,10 scientific research projects.

Li Xin, August1979, Changning county, Hengyang city, P.R. China.

Current position, grades:lecturer level of School of computer and information science in Hunan institute of technology.
University studies:MSc. of computer and communication engineering college of Hunan university.
Scientific interest: network congestion, network quality of service.
Publications: more than 5 papers.
Experience: teaching experience of 10 years, 8 scientific research projects.