View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Exeley Inc.

A Novel Key Chain-Based En-route Filtering Protocol For Wireless Sensor Networks

Zhiming Zhang[1], Xiaoyong Xiong[1], Jiangang Deng[2]

[1]School. of Software,
[2]Science and technology research place,
Jiangxi Normal University, Jiangxi, Nanchang, China.
Emails: zzm_9650@163.com

Submitted: Apr.20, 2013 ***Accepted: July 26, 2013*** ***Published: Sep.05, 2013***

Abstract- Sensor nodes may be deployed in hostile environments. An adversary may compromise the sensor nodes and inject false data into the network, which wastes scarce energy resources of the forwarding nodes. Existing schemes can effectively resist false data injection, but most of them do not consider the identifiers (IDs) attack, the en-route nodes check only the Message Authentication Codes (MACs) and do not verify the nodes identifiers (IDs) of the endorsing reports. In this paper, we propose a novel security routing protocol (KCEFP) based on one-way key chain. The proposed protocol can resist false data injection, replay and IDs attacks, and if the endorsement report is modified, the forwarding nodes can verify the endorsement report by the key chain, and filters out the fabricated packet right now. The security and performance analysis shows that our scheme provides a high security level and the energy savings significantly increasing with the number of fabricated report packet increasing.

Index terms*:* Wireless Sensor Networks, key chain, false data injection attack, different operation, fabricated packet.

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of one or multiple base stations and many sensor nodes. In Wireless sensor networks, each sensor node will monitor the surround area to sense the environment conditions, and then forward these data to the base station. By the advantage of wireless communication, the wireless sensor network can be applied in many filed such as environment monitoring, health care, virtual fences, surveillance, and military [1-3].

In many scenarios, wireless sensor networks are deployed in hostile environments, thus, secure communication is a very important requirement in wireless sensor network. Many scholars have been done much research work [12-17] on how to protect the communication security of wireless sensor networks. And because the computation, communication and power limitations of wireless sensor networks, the adversaries could easily compromise sensor nodes, and the adversary can inject the false data into the sensing data through the compromised nodes [4], the invalid data packet will be forward to the base station along the forwarding path, which can not only deceive the base station but also deplete the limited resource of wireless sensor networks. Furthermore, the adversary can launch a replay attack by sending out multiple copies of an intercepted legitimate report and waste the scarce energy of forwarding nodes. How to resist false data injection and replay attacks is very import in wireless sensor networks.

In order to resist false data injection attack in wireless sensor networks, many scholars have been done much research work [5-13]. But most of them do not consider the identifiers (IDs) attack, the en-route nodes check only the Message Authentication Codes (MAC) and do not verify the nodes identifiers (IDs) of endorsing the reports, the adversary can modify the node ID list so that the base station is not able to verify the reports, which wastes the scarce energy resources of all the forwarding nodes.

In this paper, a novel security routing protocol based on one-way key chain and different operation (KCEFP) is proposed. The proposed protocol (KCEFP) can resist false data injection, replay and IDs attacks, and if the endorsement report is modified, the forwarding nodes can verify the endorsement report by the key chain, and filters out the fabricated packet right now. The security and performance analysis shows that our scheme provides a high security level and the energy savings significantly increasing with the number of fabricated report packet increasing.

The organization of the lecture is as follows. The related work is introduced in section 2, in section 3 briefly introduces network model, assumptions and One-Way Hash key chain, the section 4 is the description of KCEFP, the security, and performance analysis of the new scheme are discussed in section 5 and 6, section 7 is the conclusion and further work.

II. RELATED WORK

In 2004, An interleaved hop-by-hop authentication scheme for filtering of injected false data was proposed by Zhu et al [5], in the scheme, to defend against false data injection attacks, at least t + 1 sensor nodes have to agree upon a report before it is sent to the base station, here the t is a security threshold based on the security requirements of the application under consideration and the network node density. Further, all the nodes that are involved in relaying the report to the base station authenticate the report in an interleaved, hop-by-hop fashion, any data change between two associated nodes was considered as false data injection. The scheme can guarantee that if no more than t nodes are compromised, the base station will detect any false data packets injected by the compromised sensors.

In [6], A Statistical en-route filtering mechanism (SEF) was proposed by F. Ye et al to detect and drop false reports during the forwarding process. In SEF, a legitimate report is generated by multiple surrounding sensors, and the legitimate report is attached endorsement nodes' message authentication codes (MACs). As a report is forwarded through multiple hops toward the sink, each forwarding node verifies the correctness of the MACs carried in the report with certain probability and drops the report if an incorrect MAC is detected. However, due to its design strategy, only a few intermediate nodes have the ability to check the validity of forwarding messages.

In 2007, Vinod Shukla and Daji Qiao proposed a secure statistical scheme (SSTF)[7], SSTF is able to distinguish transient data from false data in most scenarios, in the scheme, each sensor computes a statistical digest of the monitored phenomenon over a moving window of recent readings and reports this digest along with the current reading to CH. By utilizing the statistical digests to aid in decision making and data aggregation at the CH. But if only the current sensed readings are reported by individual sensors, it is very difficult to distinguish transient data from false data, and SSTF requires the CH to perform a series of carefully-designed inter-sensor tests

on both readings and digests reported by individual sensors, which increases the burden of the CH.

Ren Kui et al proposed a security End-to-end data transient scheme (LEDS) [8], in the LEDS, a location-aware end-to-end security framework is proposed, in which each node only stores a few secret keys and those secret keys are bound to the node's geographic location. This location-aware property successfully limits the impact of compromised nodes only to their vicinity without affecting end-to-end data security. LEDS could guarantee efficient en-route bogus data filtering and is highly robust against many know DoS attacks by one-to-many data delivery approach, but the scheme requires each node must know location information of the node.

Ozdemir.Suat et al proposed a data aggregation and authentication protocol (DAA)[9], the DAA could provide false data detection and secure data aggregation against up to T compromised sensor nodes. To detect false data injected by a data aggregator while performing data aggregation, some neighboring nodes of the data aggregator (called monitoring nodes) also perform data aggregation and compute message authentication codes (MACs) for the aggregated data to enable their pair mates to verify the data later. DAA also provides data confidentiality as data are forwarded between data aggregators. To provide data confidentiality during data forwarding between every two consecutive data aggregators, the aggregated data are encrypted at data aggregators, and false data detection is performed over the encrypted data rather than the plain data. Whenever the verification of encrypted data fails at a forwarding node, the data are dropped immediately to minimize the waste of resources such as bandwidth and battery power due to false data injection.

Yu et al. proposes a grouping-based resilient statistical en-route filtering scheme (GRSEF) for filtering false data [10]. GRSEF divide sensor nodes into T groups, which ensure any position in the monitoring area can be covered simultaneously by T nodes from distinct groups with high probability, and GRSEF introduces a multi-axis division technique to tackle the threshold limitation without relying on the sink stationarity and routing mechanism. GRSEF efficiently avoids introducing redundant groups and achieves the independence on the sink stationarity and routing protocols, but each sensor node stores a large number of keys, and the adversary only need compromise small amount nodes which can make the security protocol failure.

In [11], geographical information based false reports filtering scheme (GFFS) in sensor networks was proposed by Z. LIU and J. WANG. After deployment, each node sends its location

information to other nodes. The legitimate sensing report must carry not only MACs from t detecting nodes with distinct key partitions, but also locations of these nodes. Each en-node checks not only the correctness of the MAC and the locations carried in the report, but also the legitimacy of the locations. The scheme can resist collaborative false data injection attacks, but, obtaining the geographical information of the node depletes the sensor nodes resources.

In the schemes[5] [6] [8] [11]can resist false data injection and PDoS attacks, but do not consider the identifiers(IDs) attack, the en-route nodes check only the Message Authentication Codes(MAC) and do not verify the nodes identifiers(IDs) of endorsing the reports. the adversary can modify the node ID list so that the base station is not able to verify the reports, which wastes the scarce energy resources of all the forwarding nodes, the adversary can modify the node ID list so that the base station is not able to verify the reports, which wastes the scarce energy resources of all the forwarding nodes.

III. NETWORK MODEL, ASSUMPTIONS AND ONE-WAY HASH KEY CHAIN

a. Network Model

We consider that the wireless sensor network consists of a base station (BS) and a large amount of sensor nodes. The sensor nodes are grouped into distinct clusters after deployment. There are many clustering algorithm in wireless sensor networks [18-19], we use the cluster algorithm similar to that used in scheme [19]. Once an event occurs in an area, it can be detected by many nodes in the cluster covering the area. We assume that the neighbor nodes can sense the same message. In each cluster, the cluster head (CH) collects the message receives from the detecting nodes and generates a final report, the final report is then forwarded to the base station.

b. Assumptions

We assume that nodes are limited in their storage, computational, and communication resource, the base station is not resource constrained, and is assumed to be uncompromised at all times. It is assumed that an adversary can launch many attacks. If a sensor node is compromised, all the information it holds will be known to the adversary, and the adversary can use the compromised node to inject false reports into the network, which will deceive the base station and deplete the resources of the forwarding nodes. The adversary can perform a replay attack by sending out multiple copies of an intercepted legitimate report. Furthermore the adversary can launch the

identifiers (IDs) attack; the adversary can modify the node ID list so that the base station is not able to verify the reports, which wastes the scarce energy resources of all the forwarding nodes.

c. One-Way Hash key chain

A one-way function H which maps an arbitrary length message M to a fixed-length hash value D, it is a public function easy to compute but computationally infeasible to revert, Given M and H(M) it is hard to find a message M'≠M such that H(M')==H(M).

The one-way hash key chain [6] is constructed by repeatedly applying the one-way hash function H, on a random seed number R for *m* times. For example, if let K_m=R, then K_{m-1}= H(K_m)=H^1(R) , K_{m-2}= H(K_{m-1})=H^2(R), …, K_1= H(K_2)=H^{m-1}(R), K_0= H(K_1)=H^m(R), the last hashed output(K_0) is called committed value of hash chain. So we have K_0 = H^m(K_m) =H^m(R). Given an existing authenticated element of a one-way hash chain, it can verify elements later in the sequence of use within the chain. For example, given authenticated K_i value, a node can authenticate K_{i+3} by computing H (H (H (K_{i+3}))) and verifying that the resulting value equals K_i.

IV. DESCRIPTION OF KCEFP

a. Notations

We assume that the nodes send message to the base station according to the base station's query message. Since many notations are used in our proposed protocol, in order to easy to inquire, compare and reference, we list the notations used in proposed protocol in table 1.

Table 1: Notations of proposed protocol

Notation	**Definition**
R	One big prime
H(.)	A collision-resistant one-way hash function
ID_i	The identity of the node i
BS	The base station
CH_i	the cluster head i
S_i	the node i
$K_{i,BS}$	The secret key shared between the node i and base station

$K_{CHi,BS}$	The secret key shared between base station and the cluster head i
E(K,M)	A message M encrypted with the key k
MAC	Message Authentication Codes
QUERYID	An unique query identity from base station to sensor node
T	A timestamp
||	The concatenation operation
$\oplus$	Exclusive or operation

The proposed protocol consists of five phases: System Deployment and Initialization, Query from base station, Report collection and generation, En-route filtering, and Verification.

b. System Deployment and Initialization

1) The system randomly selects a number ID_i as the unique identity of the node i.

2) Each sensor node saves a secret key shared between the node i and base station.

3) Each sensor node saves a collision-resistant one-way hash function.

4) The system deploys the sensor nodes to the target area.

5) After deploying, the sensor nodes are grouped into clusters, and a cluster head (CH) is elected in each cluster.

c. Query from base station

When the base station wants to get some message from the cluster i, it sends a query message to the cluster head i as following:

1) The base station selects randomly a big prime R as K_m from the finite field.

2) The base station computes the $K_{m-1}= H(K_m)=H^1(R)$.

3) The base station generates the query message packet, <QUERYID, K_{m-1}, $E(K_{CHi,BS}, Q||m||R||T)$ >, and sends this packet to the CH_i. The Q denotes the query message and m denotes the hops between the base station and CH_i.

4) After receiving the query message packet, the fist hop intermediate node stores the (QUERYID, K_{m-1}) to the memory.

5) And computes $K_{m-2}= H(K_{m-1})=H^2(R)$, and generates the new query message packet, <QUERYID, K_{m-2}, $E(K_{CHi,BS}, Q||m||R||T)$ >, and sends this packet to the next hop intermediate node.

6) When the intermediate node i receives the query message packet, it stores the (QUERYID, K_{m-i}) to the memory, and computes $K_{m-i-1}= H(K_{m-i})$, and generates the new query message packet,

<QUERYID, K_{m-i-1}, E($K_{CHi,BS}$, Q||m||R||T)>, and sends this packet to the next hop intermediate node. For example, in Figure.1, the hops m is 5 between the BS and CH_i, and the hash keys stored in node S_1 , S_2, S_3, S_3 and CH_i are $K_4= H^1(R)$, $K_3= H^2(R)$, $K_2= H^3(R)$, $K_1= H^4(R)$, $K_0= H^5(R)$.

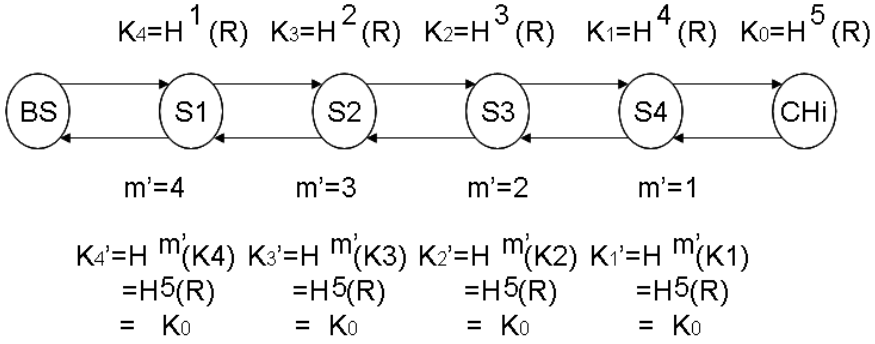

Figure 1. An example of the one-way hash key stored in the forwarding node, and the hash key computing in response phase

d. Report Collection and Generation

1) When the CH_i receives the query message packet <QUERYID, K_0, E($K_{CHi,BS}$, Q||m||R||T)>, it decrypts the message E($K_{CHi,BS}$, Q||m||R||T) by the secret key $K_{CHi,bs}$, if the T is under the reasonable ranges, the CH_i will generates the report RP according to the query message Q.

2) The CH_i sends the RP and the query message Q to his member nodes i (i=1…n), n denotes the number of member nodes.

3) After receiving the message, each the member node i generates a report RP' according to the query message Q and checks if the RP' == RP, if yes, the node i calculates MAC_i =E($K_{i,bs}$, RP), and sends the MAC_i and the identity of the node i ID_i to the CH_i.

$S_i \rightarrow CH_i$: < MAC_i, ID_i >

4) After collection at least t+1 endorsements of the report RP from his member nodes, the CH_i randomly selects t endorsements form the received endorsements, and calculates SMAC= $MAC_{CH} \oplus MAC_1 \ldots \oplus MAC_t$ = E($K_{CHi,bs}$, RP) $\oplus$ E($K_{1,bs}$, RP)… $\oplus$ E($K_{t,bs}$, RP).

5) Set m'=1, and comuptes MAC= E (K_0, ID_{CHi}||ID_1||…||ID_t||SMAC).

6) The CH_i generates report packet <(QUERYID, m', ID_{CHi}, ID_1 ,…, ID_t), SMAC, MAC, E($K_{CHi,bs}$, RP||T')>, and sends this packet to the base station along the reversed query message path, when the packet is forwarded one time, set m'=m'+1.

$CH_i \rightarrow$BS: <(QUERYID, m', ID_{CHi}, ID_1 ,…, ID_t), SMAC, MAC, E($K_{CHi,bs}$, RP||T')>

e. En-route Filtering

When all intermediate nodes receive the report packet, each intermediate node performers the step as following:

1) Each intermediate node i check if it has stored the unique identity QUERYID, if not, the packet will be dropped.

2) Otherwise, the intermediate node i get K_i from the its memory, and calculates the one-way hash key on K_i by repeatedly applying the one-way hash function H m' times, and get the hash key $K_i'=H^{m'}(K_i)= K_0$. For example, in fig.1, the hops m is 5 between the BS and CH_i, the node S_4 get the value m'=1, and computes $K_1'=H^{m'}(K_i)= H^1(K_1)= H^1(H^4(R))= H^5(R)= K_0$.

3) the intermediate node i comuptes $MAC'= E(K_i', ID_{CHi}||ID_1||\ldots||ID_t||SMAC)$ with the K_i', ID_{CHi}, ID_1 ,…, ID_t , and SMAC.

4) the intermediate node i verify if the MAC'= = MAC, if not, the packet will be dropped, because the m', ID_{CHi}, ID_1 ,…, ID_t , or SMAC is modified by adversary.

5) Otherwise, the intermediate node i forwards the report packet to the next intermediate node, and deletes the (QUERYID, K_i) from its memory.

f. BS Verification

After receiving the report packet form the CH_i, the BS will verify the valid of the report RP as following:

1) The BS decrypts the message $E(K_{CHi,bs}, RP||T')$ by the secret key $K_{CHi,bs}$, gets RP and T'. If the T' is out of the reasonable ranges, BS will drop the report packet.

2) The BS looks up the secret keys $K_{CHi,bs}$, $K_{1,bs}$,…, and $K_{t,bs}$ according to the ID_{CHi}, ID_1 ,…, and ID_t, which shared between the node i and base station.

3) The BS computes $SMAC'=E(K_{CHi,bs}, RP) \oplus E(K_{1,bs}, RP)\ldots \oplus E(K_{t,bs}, RP)$ with the share key $K_{CHi,bs}$, $K_{1,bs}$,…, $K_{t,bs}$ between the nodes and the base station.

4) The BS checks if SMAC'= = SMAC, if yes, BS receives the report packet, otherwise, BS drops the report packet.

V. THE SECURITY ANALYSIS

a. Data Confidentiality

When the outside adversary obtains the report packet of the CHi sends to the base station, it can get SMAC and E(KCHi,bs, RP||T2) , but it has no the secret share keys K1,bs,…, Kt,bs, and KCHi,bs, it can not decrypt the message E(KCHi,bs, RP||T') and SMAC, and can not obtain the report RP, so this scheme can ensures data confidentiality.

b. Resilience against false data injection attack

When the outside adversary obtains the report packet <(QUERYID, m', ID_{CHi}, ID_1 ,…, ID_t), SMAC, MAC, E($K_{CHi,bs}$, RP||T')>, it can not modify any message of the report packet to deceive the base station, because it has no the secret share keys $K_{1,bs}$,…, $K_{t,bs}$, and $K_{CHi,bs}$, between the nodes i, CH_i and the base station.

If the adversary compromises less than t nodes, t denotes the number of the CH_i member nodes. The compromised node i can generate a false data MAC_i', and sends (MAC_i', ID_i) to CH_i, the CH_i will generate SMAC', and sends report packet to the base station, it will be detected after the base station carries out verification algorithm.

c. Resilience against identifiers (IDs) attack

In the schemes [5] [6] [8] [11] can resist false data injection attacks but do not consider the identifiers (IDs) attack. In these schemes, the en-route nodes do not check the identifiers of the sensor nodes endorsing the reports, only the BS can verify the node identifiers, which make the adversary can simply modify the node identifiers list, and the BS can not correctly verify the report packet. To fight again identifiers (IDs) attack, in our scheme, the node identifiers are included in the MAC contents, each intermediate node i verify if the MAC'= = MAC, if not, the packet will be dropped, because the m', ID_{CHi}, ID_1 ,…, ID_t , or SMAC is modified by adversary.

d. Resilience against replay attack

In the query from BS phase, each intermediate nodes i store the (QUERYID, Ki) to the memory, and the intermediate nodes will delete the (QUERYID, Ki) after the report packet is forwarded or the report packet does not arrive within a certain period of time. After receiving a report packet, each intermediate node i will check if it has stored the unique identity QUERYID, if not, the packet will be dropped, so the adversary can not launch the replay attack by sending multiple copies of legitimate report packet.

VI. THE PERFORMANCE ANALYSIS

a. Storage Requirements

In this part, we show storage requirements. We assume that the base station has unlimited computation ability and storage, we do not consider the memory cost of the base station.

In our scheme, each sensor node must save the node's own identity ID_i and $K_{i,BS}$ to his memory in System deployment and initialization phase. Each node needs save (QUERYID, K_i) to his memory in the phase of query from base station. Let L_{ID}, L_{key}, $L_{QUERYID}$, and L_{Ki} denote the length of the node identity, $K_{i,BS}$, QUERYID and K_i. The storage requirements RS for a sensor node are: RS= L_{ID}+ L_{key}+$L_{QUERYID}$+L_{Ki}, suppose the length of a node identity and $L_{QUERYID}$ is 10 bits, the length of hash value and the security key is 64bits, the storage requirements RS for a sensor node is RS=10+64+10+64=148Bits=18.5bytes.

In[5], each nodes needs store the share key K_u between node u and the base station, the share pair wise key K_{uv} between nodes u and v, node u's authentication key K_u^a , and the id list of cluster acknowledgment. Let L_{ID}, and t denote the length of a node identity and the node identifiers numbers in the id list. Let L_{key} denotes the length of K_u, K_{uv} and K_u^a.The storage requirements RS' for a sensor node are: RS'= t*L_{ID}+ 3*L_{key}, suppose the length of a node identity is 10 bits, the length of the security key is 64bits, the node identifiers numbers is 10, the storage requirements RS' for a sensor node is RS'=10*10+3*64=292Bits=36.5bytes.

In [8], each nodes needs store two unique secret keys shared between the node and the sink and used to provide node-to-sink authentication, a cell key shared with other nodes in the same cell, a set of authentication keys shared with the nodes in its report-auth cells, and each sensor node is preloaded with the following bootstrapping parameters before network deployment:{K^I_M,K^{II}_M, l, (x_0, y_0), (t, T), p}. K^I_M,K^{II}_M denote two master secret keys, l and (x_0, y_0) denote and cell size l and reference point (x0, y0), The three parameters T, t, and p denote the number of endorsements included in an event report, the minimum number of endorsements to validate an event report, and a large prime. Let L_{key} , m denotes the length of secret keys and the node numbers in its report-auth cells, let L_l, $L_{x,y}$, L_t, L_T, L_p denote the length of l, (x_0, y_0), (t, T), p. The storage requirements RS'' for a sensor node are: RS''= 3*L_{key}+m* L_{key}+ L_l+$L_{x,y}$,+L_t+L_T+L_p. suppose m is 10, the length of the security key and L_p are 64bits, the length of L_l, $L_{x,y}$, L_t, and L_T are 10bits, the storage requirements RS'' for a sensor node is RS''=3*64+10*64+4*10+64=936Bits=117bytes.

The requirement analysis shows that the storage requirement of our scheme is lower than others schemes.

b. Energy Consumption

In this part, we will analysis the energy consumption of our scheme and the other scheme. We use the analysis model similar to that used in scheme [6]. Let t denotes the number of the sensor nodes endorsing the reports, let L_{ID}, $L_{QUERYID}$, $L_{m'}$, L_M denote the length of the node identity, the QUERYID, the m' value and MAC, let L_E denote the length of a report by encrypted. In our scheme, energy consumption of sensor nodes mainly is to receive and send the report packet. The format of the report packet is <(QUERYID, m', ID_{CHi}, ID_1 ,…, ID_t), SMAC, MAC, E($K_{CHi,bs}$, RP||T')>. So, the length of a report packet is $L= L_{QUERYID}+ L_m + L_{ID}*t +2*L_M+ L_E$. When a intermediate node receives a report packet from another node, a fabricated report packet will be drop after verifying, and the legitimate report packet will be forwarded, thus, the energy consumption in our scheme is $E_t=n*(L *(e_r+e_s)+e_v)+m*(L*(e_r)+e_v)$, where n, m denote the average number of hops and the number of fabricated report packet, the e_r,e_s, denote the energy consumption of receiving and sending 1 byte report packet, the e_v denotes the energy consumption of MAC computation to verify a report packet. Without our scheme, all the packet, include the legitimate and fabricated packet, will be forwarded to the base station along all the hops, let the L_r=24bytes denotes the length of a regular report, therefore, the energy consumption without our scheme is $E_r= n* L_r *(e_r+e_s)(1+m)$.

c. Simulation

We deployed randomly 2500 sensor nodes in an area of 100m × 100m, it assumed that the sensors can not move after deploying. We set the number of fabricated report packet from 1 to 10, and let n=50, t=5, e_r=12.5μJ, e_s=16.25μJ, e_v=15μJ, $L_{QUERYID}$=10Bits, $L_{m'}$=10Bits, L_M=64Bits, L_{ID}=10Bits, L_E=64Bits. In figure 2, it depicts the energy consumption for report packet forwarding with the number of fabricated report packet increasing with and without our scheme. The figure2 also gives the result of SEF [6] with the number of fabricated report packet increasing.

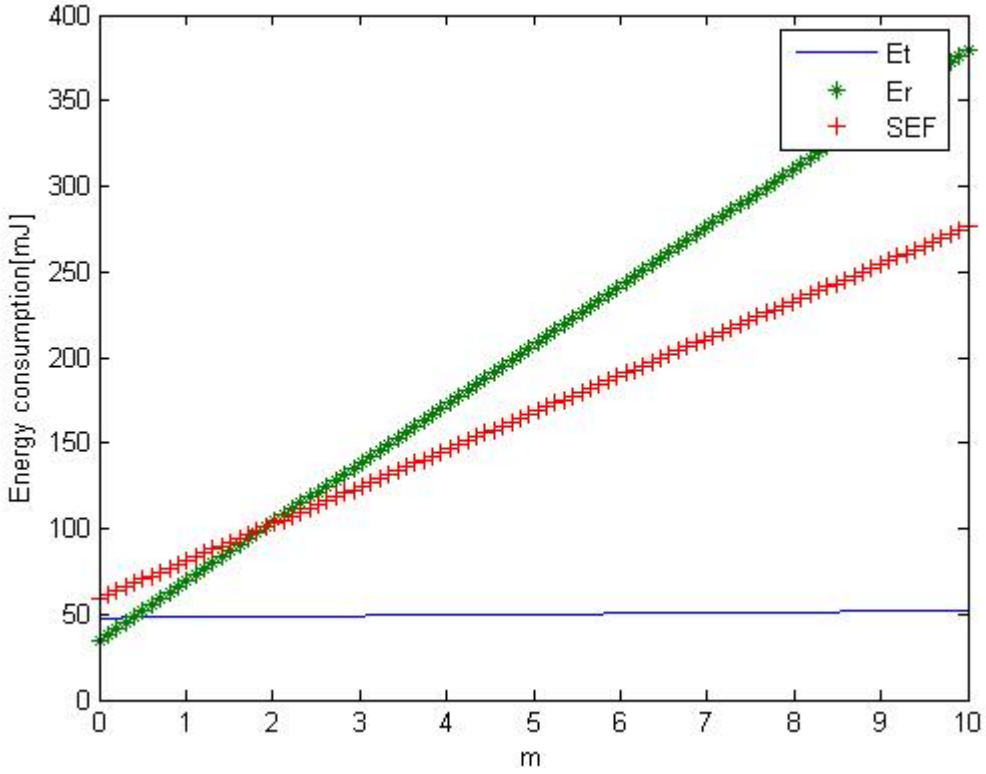

Figure 2. The energy consumption of SEF, our scheme and without our scheme

In figure2, it shows that our scheme is more efficient in energy savings than SEF with the number of fabricated report packet increasing, and it shows that our scheme starts to save energy when the amount of fabricated report packet exceeds the one report packet, and with the number of fabricated report packet increasing, the energy savings significantly increasing also. For example, when m=3, our scheme saves 1- $E_t/E_r \leqq 64.4\%$ of energy than the scheme without using our scheme.

VII. CONCLUSION

In this paper, we presented a false data injection-resilient security routing protocol based on one-way key chain and different operation. We introduced a lightweight Encryption system one-way key chain which is applied in resource constrained wireless sensor networks. Each en-route nodes can verify the report packet through checking the validity of the one-way hash key value, if the hash key value is invalid, the false report packet can be filtered out immediately. The security and

performance analysis shows that our scheme can resist false data injection, replay and IDs attacks, and the storage requirement is lower than the others scheme. Furthermore, the energy savings significantly increasing with the number of fabricated report packet increasing.

ACKNOWLEDGEMENTS

This work was financially supported by the Major International Joint Research Program of China (2010DFB90460) and supported by National Natural Science Foundation of China (61363077).

REFERENCES

[1] Ren F Y, Huang H N, Lin C, “Wireless sensor networks”, Journal of Software, 14(7), 2003, pp. 1282-1291.

[2] T. K. Dakhlallah, M. A. Zohdy and O.M. Salim， “Type-2 Fuzzy Kalman Hybrid Application for Dynamic Security Monitoring Systems based on Multiple Sensor Fusion”, International Journal On Smart Sensing and Intelligent Systems, VOL. 4, NO. 4, 2011, pp. 607-29.

[3] CUI L, JU H L, MIAO Y, “Oveview of wireless sensor networks”, Journal of Computer Researcher and Development, 42(1), 2005, pp. 163-174.

[4] Su Z, Lin C, Feng F J, et al, “Key management schemes and protocols for wireless sensor networks”, Journal of Software, 18(5), 2007, pp. 1218-1231.

[5 S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks”, In IEEE Proceedings of Symposium on Security and Privacy, 2004, pp. 259-271.

[6] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route Filtering of injected false data in sensor networks”, In:Proc. Of the 23rd annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2004), Hong Kong: IEEE Press, 2004, pp. 2446-2457.

[7] Vinod Shukla and Daji Qiao, “Distinguishing Data Transience from False Injection in Sensor Networks”, 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON, 2007, pp. 41-50.

[8] Ren. Kui, Lou.Wenjing, Zhang.Yanchao, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks", IEEE Transactions on Mobile Computing, v7, n5, 2008, pp. 585-598.

[9] Ozdemir.Suat, Çam, Hasan, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks", IEEE/ACM Transactions on Networking, v18, n3, June 2010, pp. 736-749.

[10] Yu L， Li J, "Grouping- based Resilient Statistical En-route Filtering for Sensor Networks", IEEE INFOCOM, 2009, pp. 1782-1790.

[11] LIU Zhi-xiong, WANG Jian-xin, "Geographical information based false report filtering scheme in wireless sensor networks", Journal on Communications, 33(2), 2012, pp. 156-163.

[12] Zhiming Zhang, Changgen Jiang, Jiangang Deng, "A Secure Anonymous Path Routing Protocol for Wireless Sensor Networks", 2010 IEEE International Conference on Wireless Communications, Networking and Information Security. Beijing, China, 25-27 June 2010, pp. 415- 418.

[13] Vasanth Iyer, Garimella Ram Murthy, and M.B. Srinivas, "Training Data Compression Algorithms and Reliability in Large Wireless Sensor Networks", International Journal On Smart Sensing and Intelligent Systems,VOL. 1, NO. 4, 2008, pp. 912-921.

[14] Zhimin Li, Xin Xu, Zexiang Fan, " Lightweight Trusted ID-based Signcryption Scheme for Wireless Sensor Networks", International Journal On Smart Sensing and Intelligent Systems, VOL. 5, NO. 4, 2012, pp. 799 – 810.

[15] Zhang Zhiming, Chen Deqiao, Jiang Changgen, "A Hierarchical Secure Reliable Routing Protocol for Wireless Sensor Networks", Sensor letters. vol.9, No.4, 2011, pp. 1561-1565.

[16] Jun XU , Xuehai ZHOU, Feng YANG, " Traceback in wireless sensor networks with packet marking and logging", Front. Comput. Sci. China, 5(3), 2011, pp. 308–315.

[17] Muhammad Shoaib Siddiqui, Syed Obaid Amin and Choong Seon Hong. "Hop-by-Hop Traceback in Wireless sensor networks," IEEE communications letters.VOL.16, NO.2, February 2012, pp. 242-245.

[18] A. A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks", In Computer Communications, 30(14), 2007, pp. 2826-2841.

[19] A. F. Salami, H. Bello-Salau, F. Anwar1, A. M. Aibinu, "A Novel Biased Energy Distribution (BED) Technique for Cluster-Based Routing in Wireless Sensor Networks",

International Journal On Smart Sensing and Intelligent Systems, VOL. 4, NO. 2, 2011, pp. 161 – 173.