ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

Authentication Provision for WSN Based On Multilevel Security

Shamna Hameed, Liliya.T.Jose

PG Scholar, Dept of CSE, Vimal Jyothi Engineering College, Kannur, Kerala, India

Assistant Professor, Dept of CSE, Vimal Jyothi Engineering College, Kannur, Kerala, India

ABSTRACT: Mobile sinks are the essential components in the operation of many sensor network applications.It plays a vital role in many wireless sensor network applications for efficient data accumulation, localized sensor reprogramming, for distinguishing and revoking compromised sensors. The problem of authentication and pair wise key establishment in sensor networks with mobile sink is still not solved in the mobile sink replication attacks The attacker can easily take a control of the entire network by deploying a replicated mobile sinks. So that more computational cost and the life time of sensors are reduced. In order to overcome such a problem a multilevel security scheme is introduced to perform against the mobile sink replication attack. So the identification and isolation of replicated mobile sink from network is done by adding a destination sequence number along with mobile sink request message.This destination sequence number is known only to the source node.The source node receiving the mobile sink request message will detect whether the request is from the genuine mobile sink or the replicated one.The destination sequence number of 32bits consisits of two parts. First part is of counting the sequence of request message and the second part is to recognize whether request message is from the corresponding mobile sink.Whatever the number of second part be,the value of the first part is in the increasing order.The second part is assigned by a hash function,the first part and the MAC address of the node.The hash function can generate 160bits hash value by using MAC address of the mobile sink.The source node knows the MAC address of all the nodes in advance.To reduce the overhead of detecting the replicated mobile sink one byte of hash value is selected to determine the second part in each request message generation.Thus the throughput of the entire network is maintained whenever a replicated mobile sink sends request to the source node.Also the probabaility of number of compromised nodes decreases during the mobile sink replication attack.The requested data is being preserved from the requested source node to the replicated mobile sink. The throughput remains the same with genuine mobile sink having no increase with the amount of request send by the replicated mobile sink after the genunine mobile sink had sent the request.So that the mobile sink replication attack is maintained in the enhanced multilevel security scheme using the destination *sequence number*.

KEYWORDS*:* Security, key management, wireless sensor networks, Destination sequence number

I. INTRODUCTION

The WSN[1] consists of wide distributed sensors to monitor physical or environmental conditionssuch as temperature, sound, pressure, etc. and to pass their data through the network to a destination. The advancement of wireless communication technologies and rooted computing, are being widely adapted into many applications through sensor networks and many active researches on related subject are being carried out. Several sensor nodes are connected to build the wireless sensor networks. The large number of small autonomous devices are embedded in the sensors which are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

interconnected to form sensor networks. The most formidable attack in wireless sensor network is the replication attack. The attacker compromises a node and uses its secret cryptographic key materials to effectively colonize the network with the clones of it. The replication attack is carried in two ways: mobile sink replication attack and stationary access node replication attack. There are some solutions available for stationary access point replication attack compare with mobile sink replication attack. Many important functions of the sensor network such as routing, resource allocation, misbehaviour detection, network resilience, throughput etc are remarkably injurious by replication attack. The above problem of replication attack can be solved through polynomial pool pre distribution scheme.

There are number of key pre distribution schemes[2] for solving the problem of authentication and pair wise key distribution which do not exhibit desirable network resilience The new security challenge for data collection is by avocation of pair wise key establishment and authentication in the mobile sinks. In the basic probabilistic and q-composite key pre distribution schemes, the attacker gain the control of entire network by deploying a replicated mobile sink preloaded with some compromised keys. Those compromised keys can be achieved by an attacker by obtaining large number of keys by capturing a small fraction of nodes. So for that a pair wise key pre distribution scheme that provide authentication and pair wise key establishment amid sensor nodes and Mobile Sink. A general three-tier security scheme is established for authentication and pair wise key establishment, based on the polynomial pool based key pre distribution scheme. In polynomial pool-based key pre distribution scheme both mobile sink and stationary access nodes generates the separate subset of keys which results in the high computational cost. In order to overcome this problem Random pair wise pre distribution scheme is used to reduce the computational cost and provides security against the replication attacks in the proposed system. In Random pair wise pre distribution scheme only mobile sink generates a key with key identifiers and broadcasted to stationary access nodes and sensor node.

II. RELATED WORKS AND DRAWBACKS

A randomly chosen sensor nodes called stationary access nodes authenticates the mobile sink request message to the sensor nodes. The scheme is said to be the three tier security scheme[3] in which the sensor nodes is being triggered to provide the necessary data required by the mobile sink.The scheme uses two separate polynomial pools: static polynomial pool and mobile sink polynomial pool. Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes. Rather, the attacker would also have to capture sensor nodes that carry keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication, and thus, to gain access to the network for data gathering.

The scheme is divided into two stages: static and mobile polynomial predistribution and key discovery between a mobile sink and a sensor node.

Stage 1(Static and mobile polynomial predistribution).

This is performed before the nodes are deployed. A mobile polynomial pool and a static polynomial pool are generated along with the polynomial identifiers .A mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured.

Stage 2(Key Discovery between a Mobile Sink and a Sensor Node)

To establish a direct pair wise key[4] between sensor node and mobile sink, a sensor node needs to find a stationary access node in its neighbourhood, such that, node a can establish pair wise keys with both mobile sink and sensor node. If a direct secure path establishment is there between sensor nodes and mobile sink, then the mobile sink sends the pair wise

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

key to stationary access node in message encrypted and authenticated with the shared pair wise key ;access nodes between mobile sink and access nodes. If access node receives the above message and it shares a pair wise key with sensor node, it sends the pair wise key to sensor node in a message encrypted and authenticated with pair wise key; sensor node between access node and sensor node.

To perform a stationary access node replication attack on a network, the adversary compromises at least a single polynomial from the static pool. This can be obtained easily by capturing arbitrary sensor nodes in the network. Then, the adversary can make use of this compromised polynomial by a replicated stationary access node to enable insecure access to the network. When successful access to the network has been obtained through the compromised static polynomial, the replicated stationary access node transmits recorded mobile sink data request messages. So that the nodes that have the compromised polynomial in their rings will insecurely authenticate and establish a pairwise key with the replcated node and thus deliver their data to the replicated node.

The remedy for security performance is done by using a one-way hash chain algorithm in conjunction with the polynomial pool scheme. In addition to the static polynomial, a pool of randomly generated passwords is used to enhance the authentication between sensor nodes and stationary access nodes.

Both the sensor nodes and the stationary access node with randomly select a password from the password pool along with the polynomial keys for authentication.Each password is blinded with the use of a collision-resistant hash function such as MD5 [5]. Due to the collision-resistant property, it is computationally infeasible for an attacker to find the password by its hash values. To establish an authentication between a sensor node and a stationary access node they must share common key as well as in the access node verification, to verify the authenticity of a stationary access node, the sensor node performs a single hash operation on the hash value that is sent from the stationary access node.

To perform the mobile sink replication attack the adversary has to compromise at least one polynomial from the mobile polynomial pool. To achieve this, the adversary must capture at least a specific number of stationary access nodes that hold the same mobile polynomial. It follows from the security analysis of the Blundo scheme.But this doesnot provide much resilence against the mobile sink replication attack in the network. It doesnot provide better performance in the security area of the multilevel based security scheme using the mobile sink. Also the number of keys compromised exceeds in the case of mobile sink replication attack in the network.

III. ENHANCED SCHEME USING DESTINATION SEQUENCE NUMBER

The mobile sink replication attack is made to be resilient in the network by adding an additional destination sequence number along with the request message send by the mobile sink.The key function in detecting the replicated mobile sink is how to generate destination sequence numbers and check whether receiving messages invalid or not. The 32bits destination sequence number will be divided into two parts,the first part has number of a bits and the other part occupied number of b bits. The first number of a bits is used to count sequence of generatingrequest message from the mobile sink. The second part is designed to recognize whether the request message is from corresponding detection node by a hash function. Whatever the number of second part is, the value of first part is in increasing order. Therefore the 32 bits destination sequence number composed of a bits and b bits in request message will be also in increasing order.

The MAC address of the destination node that is the mobile sink is known in advance by the sensor node.So that whenever the request reaches the sensor node it will perform a hash function on that MAC address to know the valid request.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

The second part of the destination sequence number consists of constants defined by the parts of the MAC address along with the rightmost bytes selected from the hash value generated by applying SHA-1 hash function in the MAC address.

Such a sequence number is send by the mobile sink,So that the sensor node performs the hash function and finds the MAC address that is the second part in the destination sequence number.If it is the valid mobile sink then only the requested message will be forwarded by the source sensor node.Otherwise the mobile sink is said to be duplicated or replicated in the network thus enabling the detection of the mobile sink replication attack in the sensor network.

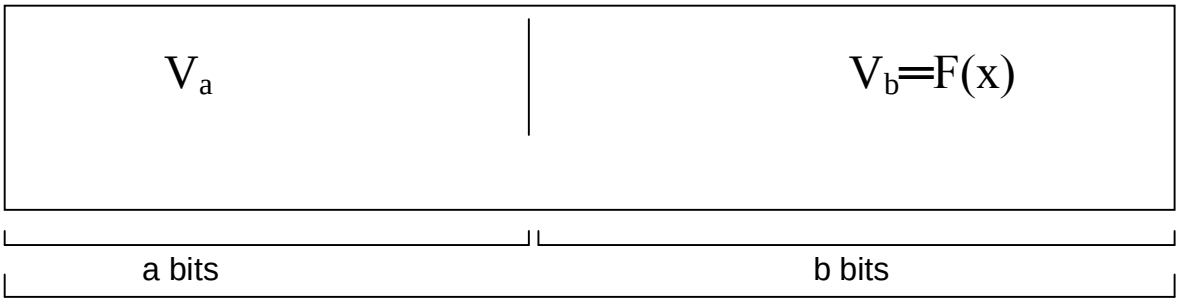

Fig-1: Division of Destination sequence Number

MAC Address :10-OD-A9-F4-6D-3E
A B C
SHA-1 hash function Hash_value_gen=SHA-1(10OdA9F46D3E")
Hash value=38b4b68c8d45C68846a754a647ef948950133393(160bits)
$C_r=\left[\frac{Va}{2}\right] mod 20$
X=Rightmost byte selection(Hash-value-gen,C_r)
F(x)=(A*B*X+C)mod 2^b

Fig-2: An Example of V_b in Destination Sequence number

IV. SIMULATION RESULTS

The number of compromised nodes decreases while the scheme works in a mobile sink replication attack.The throughput remains the same for the genunine nodes while it goes down in the case of the mobile sink replication attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

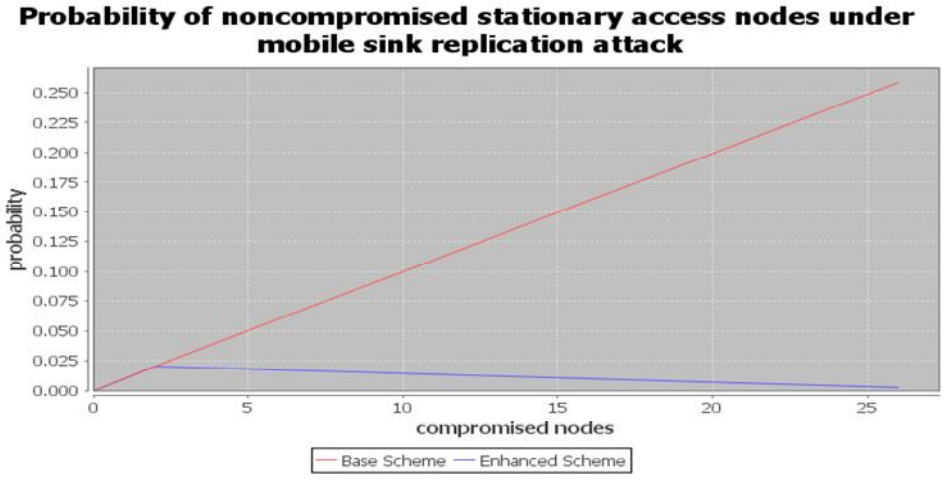

Fig-3 Probability of noncompromised stationary access nodes under mobile sink replication attack

V. CONCLUSION

The mobile sink replication attack in the network is made to get rid off by providing an additional destination sequence number that is the MAC address of the requesting mobile sink along with common key shared between the stationary access node and also along with the same password between them. Also the probabaility of number of compromised nodes decreases when the mobile sink replication attack will occur.So that the security mechanism is improved and the number of compromised keys is made to minimum.

REFERENCES

1. I.F Akyildiz, W.Su, Y.Sankara Subramaniam and E.Cayicri,"Wireless Sensor Networks:A Survey," Computer Networks,vol.38,no.4,pp.393-422,2002
2. H.Chan,A.Perrig and D.Seng,"Random key Pre distribution schemes for Sensor networks" Proc.IEEE Symp.research in Security and Privacy,2003
3. Amar Rasheed,Rabi Mahapatra.N,"The Three-tier security scheme in Wireless sensor Networks with Mobile Sinks",IEEE Transactions on Parallel and Distributed Systems,IEEE Computer society,Vol.23,No.5,pp 958-965,2012
4. D.Liu,P.Ning and R.li."Establishing pairwise keys in distributed sensor Networks",Proc.10th ACM Conf.computer and Comm.security(CSS'03),pp 52-61,Oct 2003
5. R.Rivest,"The MD5 Message Digest Algorithm",RFC 1321,Apr 1992

BIOGRAPHY

Shamna Hameed is a PG Scholar at Vimal Jyothi Engineering College, Kannur, Kerala.She is doing her final year M.Tech in Computer Science and Engineering.

Liliya.T.Jose is the Assistant Professor in Computer Science and Engineering at Vimal Jyothi Engineering College, Kannur, Kerala.