IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Wireless Network Security Framework for Mobile Sink Attack

Mr. Kaustubh K. Markande[1], Ms. Amruta Ammune[2]

PG Scholar, ME (CN) Department of Computer Network Engineering, GHRCEM, Ahmednagar, Maharashtra[1]

Professor, Department of Computer Engineering, GHRCEM, Ahmednagar, Maharashtra[2]

Abstract: In wireless sensor network sensor node are prohibits to computational resource and always created in hash unwanted and unattended environment. Security concern comes into picture in the form of authorization and authentication of data in wireless network. Development of wireless Sensor network has many applications such as military sensing and monitoring, health monitoring and traffic monitoring. Mobile sink is play a vital role in the wireless sensor network for data accumulation, localize, sensor programming and revoking compromising sensor node. Authentication problem and pair wise key establishment problem in wireless sensor network with mobile sink. This Framework, two separate key pool are used one for the sink node access and one for the pair wise key establishment between the between the sensor nodes for reducing attack on the network. We are used a stationary access network for authentication mechanism provide in sensor node and stationary access node as a Access point. This framework provides higher network resilience to mobile sink replication attack as compared to polynomial pool based scheme.

Keywords: Wireless Sensor Network (WSN), Mobile Sinks (Ms), Replication Attack and Polynomial Pool.

I. INTRODUCTION

In the three tier framework a small fraction of node are preselected sensor node is called as Stationary Access Node (SAN). Stationary Access Node SAN used for the authentication as a access point to the network the sensor node transmit their data to mobile sink by using the Stationary Access Node (SAN). Mobile sink send the data request message to the sensor node by using the stationary access node (SAN). Stationary access Node send data request message to triggering sensor node which transmit data to requested mobile sink. Generally, this framework used two polynomial pool for authentication and improved network resilience that is mobile polynomial pool and static polynomial pool. Using this two polynomial pool separately and few sensor node carry keys from mobile key pool so attacker not to be easy to attack launch mobile sink replication attack on network by capturing the some sensor node. Mobile sink replication attack compare single polynomial pool based key pre distribution attack. Single polynomial pool located on the Stationary Access Node (SAN). In the framework solve the key distribution and replication attack problem in wireless sensor network. Develop a three tier security scheme providing authentication and pair wise key pre distribution scheme. In the framework authentication pair wise key establishment based on the polynomial based key distribution scheme. This scheme improved to network resilience and mobile sink replication attack as compare to single polynomial pool based key pre distribution scheme many sensor nodes not be suffer from replication attack.

II. RELATED WORK

1. Linciya.T1 and Anand kumar. K.M2,"ENHANCED THREE TIER SECURITY ARCHITECTURE FOR WSN AGAINST MOBILE SINK REPLICATION ATTACKS USING MUTUALAUTHENTICATION SCHEME", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 2, April 2013

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. In q-composite key pre distribution scheme, a large number of keys are compromised by capturing a small fraction of sensor nodes by the attacker. The attacker can easily take a control of the entire network by deploying a replicated mobile sinks. Those mobile sinks which are preloaded with compromised keys are used authenticate and initiate data communication with sensor node. To determine the above problem the system adduces the three-tier security framework for authentication and pair wise key establishment between mobile sinks and sensor nodes. The previous system used the polynomial key pre distribution scheme for the sensor networks which handles sink mobility and continuous data delivery to the neighboring nodes and sinks, but this scheme makes high computational cost and reduces the life time of sensors. In order to overcome this problem a random pair wise key pre distribution scheme is suggested and further it helps to improve the network resilience. In addition to this an Identity Based Encryption is used to encrypt the data and Mutual authentication scheme is proposed for the identification and isolation of replicated mobile sink from the network.

2. Amol Magar, B.S. Sonawane, "An Efficient Security Scheme In Wireless Sensor Network With Mobile Sink", International Journal of Advance Research and Innovation Vol 7 Issue 3,2013

Sensor networks may be deployment in hostile environments, especially in military applications. Small low cost sensor devices each equipped with limited

resources are networked and are used for various critical applications. Making such sensor network secure is a challenging issue. Under such situations, the sensors may be captured, and the data may be intercepted and/or modified by the attacker. Therefore security services such as authentication and pair wise key establishment is a critical issue to maintain network operations. In the traditional schemes an attacker can easily obtain large number of keys by capturing small fraction of nodes and initiate data communication with any sensor node. Here the main focus is on the sensor network that uses mobile sink to gather the sensed data from the network. A new security technique- Three tier security scheme is proposed to provide authentication and pair wise key establishment between sensor nodes and mobile sinks. The proposed scheme makes use of two polynomials pools: static polynomial pool and mobile polynomial pool which will improve network resilience to the mobile sink replication attack.

3. T. Subramani1, S.Ravi Varma2 , R.Kabileshwaran 3," A Security Framework for Replication Attacks in Wireless Sensor Networks", International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2908-2915

Mobile sinks play a great role in many Wireless Sensor Network applications for efficient data accumulation, localized sensor reprogramming and for collecting data from various sensor nodes across the globe. However, in sensor networks that make use of the existing three tier security framework, elevates a new security challenge i.e an attacker can easily create a replicated node and can gain control of the data in the network. Although the three-tier security framework is more resilient to mobile sink replication attacks, it is weak against access point replication attacks. To reduce the damage caused by access node replication attack, strengthening the authentication mechanism between the sensors and access nodes is vital. For this purpose, the single polynomial pool is converted to a double polynomial pool for providing security over the existing system. Also, security is increased by separating the access points into two layers namely, access nodes-D and access nodes-I along with a more secure authentication mechanism called WHIRLPOOL that produces a 512 bit encrypted text using Miyaguchi-Preneel scheme of cipher text generation.Our proposed algorithm ensures the necessary security mechanism for Wireless Sensor Networks and also does not degrade the performance of quality of service.

4. Uma P, Manjula Devi TH, "An Efficient Security Scheme providing Authentication and pair wise Key distribution with mobile sink in WSNs", International Journal of Innovative researchin science , Engineering and Technology, Vol 2 Issue 5 May2013

Sensor networks may be deployment in hostile environments, especially in military applications. Small low cost sensor devices each equipped with limited resources are networked and are used for various critical applications. Making such sensor network secure is a challenging issue. Under such situations, the sensors may be captured, and the data may be intercepted and/or modified by the attacker. Therefore security services such as authentication and pair wise key establishment is a critical issue to maintain network operations. In the traditional schemes an attacker can easily obtain large number of keys by capturing small fraction of nodes and initiate data communication with any sensor node. Here the main focus is on the sensor network that uses mobile sink to gather the sensed data from the network. A new security technique- Three tier security scheme is proposed to provide authentication and pair wise key establishment between sensor nodes and mobile sinks. The proposed scheme makes use of two polynomials pools: static polynomial pool and mobile polynomial pool which will improve network resilience to the mobile sink replication attack.

5. P. Santhi1 , Md. Shakeel Ahmed2 , Sk. Mehertaj3 , T. Bharath Manohar4 ,"An Efficient Security Way of Authentication and Pair wise Key Distribution with Mobile Sinks in Wireless Sensor Networks" International Journal of Modern Engineering Research (IJMER), Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2553-2562

Wireless sensor networks (WSN) are the emerging application in many industrial and missile sector. Mobile sinks (MSs) are vital in many wireless sensor network applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. However, in sensor networks that make use of the existing key pre-distribution schemes for pairwise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge: in the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys. The proposed work, three-tier framework permits the use of any pairwise key pre-distribution scheme as its basic component. The new framework requires two separate key pools, one for the mobile sink to access the network, and one for pairwise key establishment between the sensors.

III. MOTIVATION AND CHALLENGES

In wireless sensor applications, sensor nodes transmit critical information over the network; therefore, security services, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key predistribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

The problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of mobile sink replication attacks. For the basic probabilistic and q-composite key predistribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and then initiate data communication with any sensor node.

To address the above-mentioned problem, a general framework is developed that permits the use of any pairwise key predistribution scheme as its basic component, to provide authentication and pairwise key establishment between sensor nodes and MSs. To make the three-tier security scheme more robust against a stationary access node replication attack, the authentication mechanism is strengthened between the stationary access nodes and sensor nodes using one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme.[5]

IV. PROPOSED SYSTEM

4.1 PROPOSED SYSTEM

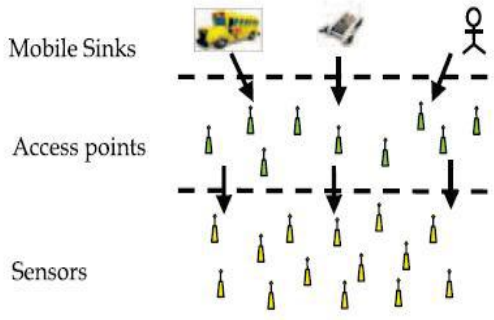

Fig4.1 Three Tier System Architecture

In the proposed technique will substantially improved network resilience to mobile sink replication attack compare to single polynomial pool based key pre distribution approach. Three Tier security framework more robust against Stationary Access Node replication attack authentication mechanism between stationary access node and sensor node using one way hash chain algorithm with static polynomial pool based scheme.[3]

In this framework used two separate polynomial pool

1. The mobile Polynomial Pool
2. The Static Polynomial Pool

4.1.1 KEY DISCOVERY BETWEEN MOBILE SINKS AND SENSOR NODES

In direct pair wise key establishment between sensor node u and mobile sink v, a sensor node u need to find a Stationary Access Node (SAN) A in its neighborhood, such that node A can establish pair wise keys with both mobile sink v and sensor node u as per Fig 4.2.1(a) shows direct secure path establishment between sensor node u and mobile sink v send pair wise key to SAN A message in the form of encrypted and authenticated share key between mobile sink v and SAN A. If node A receives the above message and it share a pair wise key with u, it sends pair wise key to node u message in the form of encrypted and authenticated with pair wise key between Sensor node u and SAN A[3]

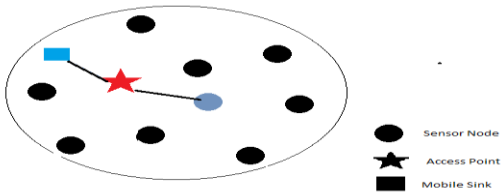

Fig 4.2.1(a) Direct Key Establishment

In indirect Key discovery through Stationary Access Node (SAN), mobile sink and sensor node will establish a pair wise key with sensor node. Establish a pair wise key with mobile sink v and a sensor node v has to find a Stationary Access Node A in its neighborhood node A can establish a pair wise key with both node u and v. if node establishes a pair wise key with only node u and not with v. Access node A can discover a common mobile polynomial with node v, sensor node u need to find intermediate sensor node (i) along the path u-i-a-v.

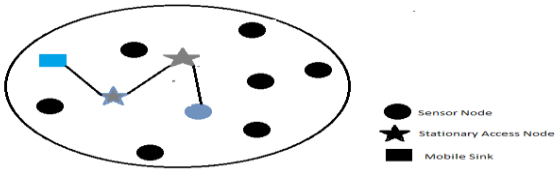

Fig: 4.2.1(b) indirect Key discovery through Stationary Access Node (SAN)

In the following figure shows that the mobile sink v and sensor node u establish a pair wise key with the help of other sensor node (i) using indirect key discovery. Establish a pair wise key with mobile sink v, sensor node u has too find stationary access node A. node A can establish a pair wise key with only node u and not with v. sensor node can discover a common polynomial with node v. sensor node u need to find intermediate sensor node i along with path u-i-A-v such that intermediate node direct pair wise key establish A.

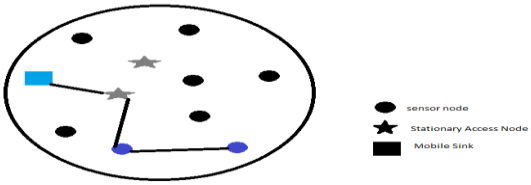

Fig 4.2.1(c) indirect key discovery through intermediate sensor node

V. ENHANCED THREE TIER SECURITY SCHEME

5.1 SPECIFICATION OF WIRELESS SENSOR NETWORK

DOI 10.17148/IJARCCE.2015.41236

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

5.1.1 Access Points

These are the intermediates in data transfer. Some of the mobile sinks act as a intermediate. They shares key from both the key pool (static and mobile). Keys from the static key pool facilities the data transfer between sensor node and access point. While the keys from mobile key pool provide authentication for the data transfer between them and the mobile sink.[4]

5.1.2 Mobile sinks

Mobile sinks informs the sensor node about their location updates, frequent change in location of the mobile sink causes to the sensor node to collide in the network. Instead of transferring the information to the entire network at each time the sink broadcast the update to local LAN.

5.1.3 Key and Key pools

Security is the important issue, in that encrypt the message sent among them so key must be mutually agreed by the communicating node. Establishing key between sensor node is challenging task key agreed scheme such as Diffle – Hellman and public key are not suitable for wireless sensor network. Key pre distribution depend upon the size of key pool and the maximum size of key pool that can be used by the scheme would be s2p, where s is the size of key pool and p is the probability that two share a common key. When the network size is large then key pre distribution not possible it consume large amount of memory. Assign a key randomly for data transmission.[4]

5.2ENHANCED THREE TIER SECURITY ARCHITECTURE

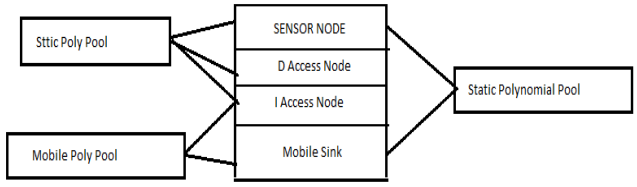

Fig 5.2Enhanced Framework Architecture

5.2.1 LAYER CONSTRUCTION

Implement of enhanced three tier security architecture in wireless sensor network three layer constructed in above namely sensor node access node and mobile sink. Transmission control protocol is used to communicate that means transmit the data between the layers. A single polynomial pool is created for communication between sensor node to access point and access point to to mobile sink.[4]

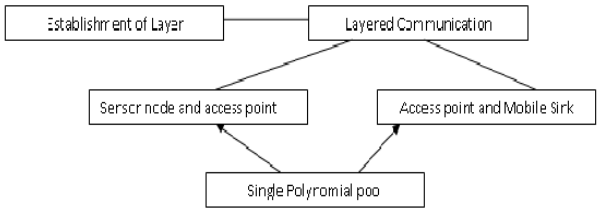

Fig 5.2.1 Layer Construction

5.2.2 KEY POOL SEGRATION

To enhance the security of framework we are crate two polynomial key pool. Generally, keys are used from static polynomial pool for data transfer between sensor node and access point and a key from a mobile polynomial pool is used for data transfer between access point and mobile sink.[4]

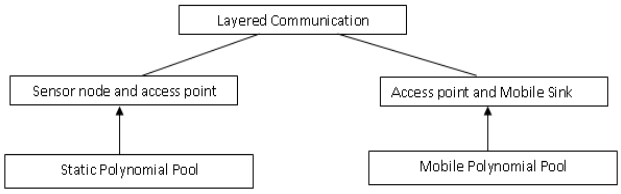

Fig: 5.2.1 Key Pool Segration

5.2.3 SECURITY ENHANCEMENT

The access point layer is separated into node with direct and indirect contact of interference range. An enhancement of advanced Encryption Standard called the Whirlpool algorithm for is used for authentication between access point and mobile sink. In layered once the segregate layer and distribute the key done by the whirlpool algorithm the probability of attack is removed attacker can not be create a replicated node and transfer the data.[4]

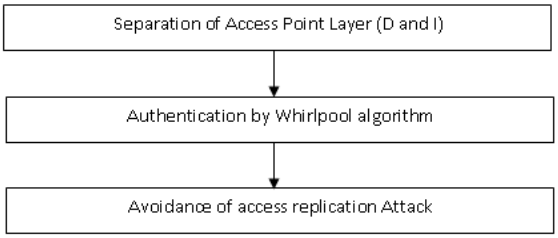

Fig: 5.2.3 Security Enhancement

5.3 WHIRLPOOL ALGORITHM

Whirlpool algorithm is designed by Vincent Rijmen and Paulo S.L.M Barreto. WHIRLPOOL is a hash function which operates on message less than 2256 bits in length and produces the message digest of 512 bits. WHIRLPOOL had three versions the first version WHIRLPOOL-0 was submitted to the NESSIE projects. WHIRLPOOL-T for the NESSIE portfolio of cryptographic primitives. Final version is simply WHIRLPOOL which adopted by ISO standard this scheme is used the 512 bit block cipher called W. the bit string to be hashed is padded with lquo “1” bit then sequence of bit “0” and finally with the original length of 256 bit, so that the length after padding is a multiple of 512 bit. The resulting string is divided into sequence of 512 bit block that is m1, m2,m3…..mt which is used to generate a sequence of intermediate hash value H0,H1,H2…….Ht. H0 is the 512 bit string of “0” bit. Compute the value of Hi, W encrypt mi using Hi-1 as key and XORs the resulting cipher text with both Hi-1 and mi. Finally the Whirlpool messages digest Ht.[4]

DOI 10.17148/IJARCCE.2015.41236

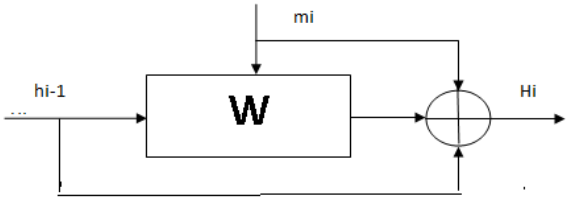

Fig: 5.3 WHIRLPOOL Algorithms

5.3.1 Initialization Function:

In the initialization function create a basic hash state for each new input value. The hashing state defines a basic structure of the hashing function.

5.3.2 Addition Function:

In addition function mark the position of the pointer in plain text. A buffer is also created. Also the data is process at a time only 8 bit. Before this step data is divided into block such a way that each block has 512 bit. The last block padded with at end as a zeroes.

1.1.1 Finalizing Function:

In this phase finally function generates 512 bit cipher text by proceeding block by block above cipher text generated by Whirlpool algorithm.[4]

VI. CONCLUSION

The proposed scheme based on polynomial pool based pre distribution scheme substantially improves network resilience to mobile sink replication attack compared to single polynomial pool based pre distribution approach. The proposed scheme is based on mobile sink server which determines the parameter such as traffic, time and bandwidth of the entire mobile sink. If the node misbehaves it revoke and assign MS randomly. Thus the replication of node and its identity can be resolved. So data collection done in secure manner.

ACKNOLEDGMENT

I like to thanks people for helping me for giving importance guidance about project work. I am very thankful to those who help me during my paper publishing as well as project dissertation stage. I am thankful to journal for giving me best opportunity to publish my paper. I am sincerely thankful to my head of department, my project guide and other staff members from department for supporting me.

REFERENCES

1. Linciya.T1 and Anand kumar. K.M2,"ENHANCED THREE TIER SECURITY ARCHITECTURE FOR WSN AGAINST MOBILE SINK REPLICATION ATTACKS USING UTUALAUTHENTICATION SCHEME", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 2, April 2013
2. Amol Magar, B.S.Sonawane, "An Effitient Security Scheme In Wireless Sensor Network With Mobile Sink", International Journal of Advance Research and InnovationVol 7 Issue 3,2013
3. T. Subramani1, S.Ravi Varma2 , R.Kabileshwaran 3," A Security Framework for Replication Attacks in Wireless Sensor Networks", International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2908-2915
4. Uma P, Manjula Devi TH, "An Efficient Security Scheme providing Authentication and pair wise Key distribution with mobile sink in WSNs", International Journal of Innovative researchin science , Engineering and Technology, Vol 2 Issue 5 May2013
5. P. Santhi1 , Md. Shakeel Ahmed2 , Sk. Mehertaj3 , T. Bharath Manohar4 ,"An Efficient Security Way of Authentication and Pair wise Key Distribution with Mobile Sinks in Wireless Sensor Networks" International Journal of Modern Engineering Research (IJMER), Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2553-2562
6. LF Akyildiz, W. Su, Y Sankarasubramaniam "Wireless Sensor Network A survey", Computer Network
7. Haowen Chan, Addrian Perrig, and Dawn Saong, "Key Distribution techniques for sensor network", Carengie Mellon University.
8. Donggang Liu, Peng Ning, "Location based pairwise key establishment for static sensor network".
9. Haowen Chan, Adreian Perrig, Dawn Sung"Random key predistribution sheme for sensor network"Donggang Liu, Peng Ning, "Establishment Pairwise key in Distributed Sensor network"
10. Tia Gao, Matt Welsh, Radford R, Juang and Alex Alm, "Vital Sign Monitoring and patient tracking over a wireless Network", 27 th Annual Conference of IEEE EMBS, Shanghai, Sept 2005.
11. Lingxua Hu, David Evans, "Using Directional to Prevent Wormhole Attack", In network and Distributed System Security Symposium, California, USA Feb 2004
12. Hongmel Deng, Wel Li, and Dharma P, P. Agrawal, "Routing Security in Wireless Adhoc Network", Telecommunication Network Security, University of Cincinnati.