A PROTOCOL IMPLEMENTATION OF SECURED WIRELESS SENSOR NETWORKS IN THE CHEMICAL INDUSTRY

[1]RUSHIKESH BHAPKAR, [2]ANJALI PATKI

[1,2]Indira College of Engineering and Management Pune, Maharashtra, India
E-mail: [1]rushikesh.bhapkar3@gmail.com

Abstract— This paper propose a bandwidth-efficient cooperative authentication scheme for filtering injected false data in Wire-less sensor Networks in Chemical Industries. Sensor node could be easily compromised as the attacker can gain control obtain key values and change the properties of the node. This results in an false report to sink and energy waste in en-route nodes. The proposed scheme can save energy by early detecting and filtering the most of injected false data with less time and difficulty at the en-route nodes. In addition, only a very small amount of injected false data needs to be checked by the sink, thereby reducing the burden on sink. To filter the false data, the proposed scheme adopts cooper-ativeneighbour router (CNR)-based filtering mechanism. Hence it achieves not only high filtering probability but also high reliability.

Index Terms— Injected false data, Wireless sensor network, compromised sensor.

I. INTRODUCTION

A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each sensor node consist of necessary data sensing, processing, and communicating components. Hence, when a sensor node generates a report on an special event, e.g., a temperature change at surrounding, will send a report to the data collection, sink through an established routing path. Various security attacks. are very vulnerable in Wireless sensor networks The most serious and dangerous one is suffering from injecting false data attack . For this injected false data attack, first several sensor node are compromised by an attacker .Therefore the attacker accesses all keying materials stored in the compromised nodes process it and send the false data to the sink . Hence a default event is triggered and report a wrong location information to the sink. One disadvantage of this attack is large no of expensive resources will be wasted as solving the huge traffic caused in a wrong location. Therefore, to filter the false data is a crucial process and it should be accurate as possible in wireless sensor networks.

In addition to the problem explained before , heavy verification burdens will fall on the sink ,as all the false data injected are flooding into the sink simultaneously, And at the same time a huge energy will be wasted at the en-route nodes in the established path. Hence what results is that, the whole wireless sensor network could be paralysed very quickly. Therefore, it is a must that filtering false data should also be executed as faster and earlier as possible in a tactful way to mitigate the energy waste at the en-route nodes and sink. Some false data filtering mechanisms have been developed to tackle this challenging issue. These existing filtering mechanisms developed use the symmetric key technique. The problem with it is the attacker in the compromised node can take advantage of its keys to generate false reports. Therefore, reliability of such filtering mechanisms will be thus degraded.

Where as the proposed mechanism resolves this problem. In this early detecting and filtering the majority of injected false data take place hence can save energy. The sink needs to verify a very small fraction of injected false data, thus largely reduces the burden of the sink. Its clear that compared with the previous mechanisms, this new mechanism achieves maximum filtering probability and high reliability.

II. LITERATURE SURVEY

In this paper A Key-Management Scheme for Distributed Sensor Networks," this scheme uses modular schemes with the property of congruence. Each sensor node store a key seed. This is used to compute a unique shared key with its cluster head and a group key shared with other nodes in the same cluster. This scheme minimises the key storage space. The sensor nodes in the network can update their key seeds faster. It also reduce time delay and energy con-sumption of key establishment. Chan propose three mechanisms for sensor networks One mechanism uses a compo-site random key pre distribution scheme. Any two sensor nodes want to establish a pairwise key. This scheme achieves high security in wireless sensor networks. Another one called Multi path key reinforcement scheme is a method to strengthen the security to set up a link key via Multi path. Let two sensor nodes P and Q want to set up a link key. Node P sends j different random values to node Q. These values are sent to Q along different paths. .The third mechanism uses a random pairwise key scheme. In this a unique random pairwise key is generated for a pair of nodes, and an ID for the node is created and also stored along with the key .Each node can find its shared common pairwise keys with its neighbours nodes using their node IDs. In the paper "TinyECC: A Configurable Library for Elliptic

Curve Cryptog-raphy in Wireless Sensor Networks" by Liu and Ning introduces two pairwise key pre distribution schemes: First a random subset assignment scheme and second a grid-based key pre distribution scheme. In the first one a server generates a set of degree polynomials. for which a unique ID is assigned. Each sensor node has a subset of these polynomials. Any two nodes that have same polynomial can set pairwise key between them directly. Others will use path key establishment method. A source node sends a request to its i forwarding nodes to establish a pairwise key with the destination node. This request will be forwarded until a node finds a path to the destination node. In the second scheme, the server assigns each enrouting node an ID and corresponding row and column polynomial. Two sensor nodes establish a pairwise key between them. If there is no match they will find a path with the help of forwarding nodes.

III. EXISTING SYSTEM

Different works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared using message authenticated code ,key binding mechanism and bit compression authentication.

A. StatisticalEn-route Filtering(SEF)

This mechanism uses Message Authenticated Code (MAC).In detection of an event each report generated by the sensor nodes validated by multiple keyed message authenticated code (MACs). As the report being forwarded, each intermediate node along the way verifies the correctness of the MACs as early as possible. Sometimes the injected false data escapes the en-routing filtering and will be delivered to the sink. In that case it will verify the correctness of each MAC carried in each report and reject false ones.

B. Interleaved hop-by-hop authentication (IHA)

In this scheme the sensor node is associated with two other forwarding nodes along the path. The one closer to the basestation is the upper associated node and the other is the lower associated node. An en-routing node will forward received report if it is correctly verified by its lower association node. Consider an example showing association where there are three sensor node. BS is the base station and CH is a cluster head. Association between two nodes is shown by an arc connected.

C. Location-Based Resilient Secrecy (LBRS)

This system adopts a location key binding mechanism. This will reduce the damage caused to node by an attacker and further reduces the false data generation in wireless sensor networks.

D. Location-aware end-to-end data security design (LEDS)

This mechanism is provide end-to-end security efficient and high data availability. LEDS uses a symmetric key and location key management, to achieve high en-routing filtering.

E. Bit-compressed authentication Technology

This technology can achieve bandwidth-efficient by compressing MAC single bit. This provide high security.

F. Limitations of Existing System

In Statistical En-route Filtering (SEF), the filtering probability at each sensor node is relatively low. It detect maximum of injected false reports. But does not consider the possibility of en-routing sensor nodes compromise. In Interleaved hop-by-hop authentication (IHA), if creation of association fails, it is vulnerable to attack.IHA use the symmetric key for authentication, which allows the compromised nodes to misuse it to generate false reports.

In Location-Based Resilient Secrecy (LBRS) and Location- aware end-to-end data security design (LEDS) requires extra overhead to achieve en-routing filtering. In LEDs all the nodes can determine their locations and generate location- based keys which take time. In Bit-compressed authentication, however, once the source is compromised, the technology does not work. Therefore, it not be used to filter false data in wireless sensor networks.

Hence in general the above mentioned existing system have various disadvantages like energy wasted in en-route nodes of wireless sensor network and also there is a heavy verification burden at sink. And finally There is no cooperative authentication among en-routing nodes.

IV. PROPOSED SYSTEM

The design goal of proposed system is to achieve bandwidth-efficient authentication for filtering injected false data. Every sensor node in wireless sensor network shares a private key with the sink. Each node knows its one-hop neighbours and establish a public-private key pair with each of them. In this scheme it use Message Authentication Code(MAC) mechanism to authenticate broadcast messages and every node can verify the broadcast messages. Each MAC is set to 1 bit to achieve bandwidth efficient authentication.

To filter the false data injected by attacked sensor nodes, the BECAN scheme adopts cooperative neighbour router (CNR)- based filtering mechanisms in figure 2 .Here a source node N0 is ready to send a report m to the sink via an established routing path PN0: {P1 – P2 ...Pl – Sink}, it first resorts to its k neighbouring sensor nodes SN0 : {S1,S2, . . .,Sk} to cooperatively authenticate the report m, and then sends it together with the authentication information MAC from N0 to the sink via routing RN0, where the

sink initialises all sensor nodes, then each one of it shares its private key with the sink.

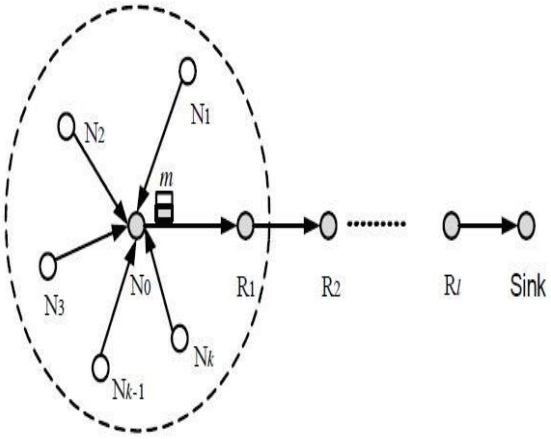

Fig. 1. Cooperative CNR-based authentication mechanism.

With this mechanism BECAN calculate the probability of k- neighbours, which provides the necessary condition needed for BECAN authentication. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes if there is at least one uncompromised neighbouring node participating in the reporting.

In addition, the accompanied authentication information is bandwidth-efficient. Finally develop a custom Java simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reportstication. Various false data filtering mechanisms have been developed, since most of these filtering mechanisms use the symmetric key technique were the compromised node can abuse its keys to generate false reports, and the reliability of the filtering mechanisms will be degraded.

The proposed mechanism can save energy by early detecting and filtering the majority of injected false data. There-fore, it is important to share the authentication tasks with the en- route sensor nodes such that the injected false data is detected and discarded earlier. If the injected false data is detected in network as soon as possible, the more energy can be saved from the whole network with only very little extra overhead at enroutenodes. Hence only small amount of injected false data needs to be verified by the head sink, which thus largely reducing its burden. Since the sensor nodes are less costlier, it is desirable to design a bandwidth efficient authentication scheme Compared with the previously reported mechanisms, this new mechanism achieves not only high filtering probability but also high reliability. i.e., even though some of the sensor nodes are compromised, obviously the actual reports generated will reach the sink with high probability

V. ALGORITHMS

Algorithm 1. Sensor Nodes Initialization Algorithm

Procedure SENSORNODESINITIALIZATION
Input: $params$ and un-initialized $\mathcal{N} = \{N_0, N_1, N_2, \ldots\}$
Output: initialized $\mathcal{N} = \{N_0, N_1, N_2, \ldots\}$
  for each sensor node $N_i \in \mathcal{N}$ **do**
    preload N_i with TinyECC, $params$ and energy
    choose a random number $x_i \in \mathbb{Z}_q^*$ as the private key, compute the public key $Y_i = x_i G$, and install (Y_i, x_i) in N_i
  end for
  return initialized $\mathcal{N} = \{N_0, N_1, N_2, \ldots, N_n\}$
end procedure

Algorithm 4. Sink Verification

procedure SINKVERIFICATION
Input: $params$, $k_{0s}, k_{1s}, \ldots, k_{ks}$, m, T
Output: *accept* or *reject*
  set returnvalue = *"accept"*
  for $i = 0$ to k **do**
    $\overline{mac}_{is} = MAC(m\|T, k_{is}, \alpha)$
    if $\overline{mac}_{is} \oplus mac_{is} \neq 0$ **then**
      set returnvalue = *"reject"*
      break
    end if
  end for
  return returnvalue
end procedure

Algorithm 2. CNR Based MAC Generation

procedure CNRBASEDMACGENERATION
Input: $params$, $N_i \in (N_{N_0} \cup N_0)$, m, T, R_{N_0}
Output: Row_i
  N_i uses the non-interactive keypair establishment to compute shared keys with each node in $R_{N_0} : [R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_l \rightarrow Sink]$ as $k_{i1}, k_{i2}, \ldots, k_{il}, k_{is}$, where k_{is} is N_i's private key distributed by the *sink*
  if N_i believes the report m is true **then** ▷ a neighboring node is assumed having the same ability to detect a true event as the source node and correctly judge the report m.
    for $j = 1$ to l **do**
      $mac_{ij} = MAC(m\|T, k_{ij}, 1)$
    end for
    $mac_{is} = MAC(m\|T, k_{is}, \alpha)$
  else
    for $j = 1$ to l **do**
      mac_{ij} is set as a random bit
    end for
    mac_{is} is set as a random bit string of length α
  end if
  return $Row_i = (mac_{i1}, mac_{i2}, \ldots, mac_{il}, mac_{is})$
end procedure

Step 3. After the source node N_0 aggregates all row vectors $(Row_0, Row_1, \ldots, Row_k)$, it formats the authentication information **MAC** as

$$\mathbf{MAC} = \begin{pmatrix} Row_0 \\ Row_1 \\ Row_2 \\ \vdots \\ Row_k \end{pmatrix} = \begin{pmatrix} mac_{01} & \cdots & mac_{0l} & mac_{0s} \\ mac_{11} & \cdots & mac_{1l} & mac_{1s} \\ mac_{21} & \cdots & mac_{2l} & mac_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ mac_{k1} & \cdots & mac_{kl} & mac_{ks} \end{pmatrix}, \quad (10)$$

and reports $(m, T, \mathbf{MAC})$ as well as N_{N_0} to the *sink* along the routing R_{N_0}.

Algorithm 3. CNR Based MAC Verification

procedure CNRBASEDMACVERIFICATION
Input: $params$, $R_j \in \{R_1, \ldots, R_l\}$, m, T, N_{N_0}
Output: *accept* or *reject*
  R_j uses the noninteractive keypair establishment to compute shared keys with each node in $\{N_0, N_1, \ldots, N_k\}$ as $k_{0j}, k_{1j}, \ldots, k_{kj}$
  set returnvalue = *"accept"*
  for $i = 0$ to k **do**
    $\overline{mac}_{ij} = MAC(m \| T, k_{ij}, 1)$
    if $\overline{mac}_{ij} \oplus mac_{ij} \neq 0$ **then**
      set returnvalue = *"reject"*
      break
    end if
  end for
  return returnvalue
end procedure

CONCLUSION

Proposed BECAN scheme for filtering the injected false data, has been demonstrated to achieve not only high en- routing filtering probability but also high reliability with multi-reports. Due to this the BECAN scheme could be applied to other fast and distributed network were the authentication purpose is also distributed, e.g., authentication function in the wireless mesh network. BECAN does not require a complex security fixation because it uses a noninteractive key establishment. In addition, BECAN considers the situation that each node could be compromised, hence it distributes the en-routing authentication information to all sensor nodes on the routing path. It also adopts the bit-compressed authentication technique to save the bandwidth. Therefore, it is very suitable for filtering false data in wireless sensor networks and hence compromise-tolerant. In our future work, we will investigate how to prevent or reduce the gang injecting false data attack from mobile compromised sensor nodes.

REFERENCES

[1] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Ninth ACM Conf. Computer and Comm. Security, 2002

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," IEEE Symp. Security and Privacy, 2004

[3] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Net-works," IEEE J. Selected Areas in Comm. 2006.

[4] K. Ren, W. Lou, Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[5] X. Lin, R. Lu, and X. Shen, "MDPA: Multidimensional Privacy- Preserving Aggregation Scheme for Wireless Sensor Networks," Wireless Comm. and Mobile Computing, 2010.

[6] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," IEEE INFOCOM '06, Apr. 2006.

[7] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," IEEE GLOBECOM 2009.

★★★