Security in Wireless Sensor Networks

Rovina D’britto
Computer Engineering Department
St. Francis Institute of Technology
Mumbai, Maharashtra

Vincy Joseph
Assistant Professor
Computer Engineering Department
St. Francis Institute of Technology
Mumbai, Maharashtra

***Abstract*— Wireless Sensor Networks (WSN) is an emerging technology and can be used in various applications for example in critical situations like battlefields and commercial applications such as vehicle tracking and detection , traffic observing , natural environment of organism, smart homes and many more scenarios. The major challenge that wireless sensor networks face today is security. Sensor nodes are deployed into unattended environment and so they are more vulnerable to variety of potential attacks. There are various attacks in wireless sensor networks from which false data injection is one of the dangerous attacks in WSN. Using en-route filtering mechanism the false data injection attack can be minimized. There are various en-route filtering schemes such as DEF, VEBEK and BECAN which allows dropping of false data. The analysis is done to find out the pros and cons of various enroute filtering techniques for false data injection attack.**

Keywords—wireless sensor network, false data injection attack, En-route filtering

I. INTRODUCTION

The design of sensor network is in real-time collection and analysis of low level data in destructive environments. For this reason they are well suitable to a large amount of monitoring and observation applications. Wireless sensor network applications include environment monitoring, fire response, military communications, manufacturing quality control, observation of critical organizations, smart houses, distributed robotics, traffic monitoring, investigating human emotions etc. Most of the sensor networks are organized in hostile environments with active intelligent opposition. Hence security is a critical issue. One obvious example is arena applications where there is a pressing need for secrecy of location and fighting to sabotage and destruction of network.

ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are weak to security attacks because of the broadcast character of the transmission standard. Wireless sensor networks also have an additional weakness because nodes are often placed in a dangerous environment where they are not actually protected. Attacks are basically classified as active attacks and passive attacks. Figure1. shows the classification of attacks on WSN.

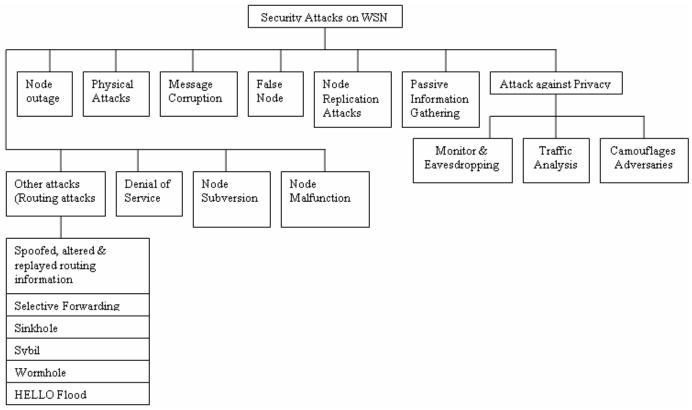


Figure1. Classification of Security Attacks on WSN [1]

A. Active Attacks

The active attacks are those in which the attacker alters, modifies the data in the communication channel.

1. Routing Attacks in Sensor Networks

The attacks which act on the network layer are called routing attacks. Attacks such as Spoofed, altered and replayed routing information can occur while routing the messages.

2. Wormhole attack

An invader records packets (or bits) at one place in the network, channels them to another location, and retransmits them into the network.

3. Denial of Service

Denial of Service (DoS) is any type of attack where the attackers attempt to prevent legitimate users from accessing the service. DoS attack is meant not only for the opponent’s attempt to destroy a network, but also for any occurrence that weakens a network’s ability to run a service.

4. Node Subversion

Capture of a node may disclose its evidence including discovery of cryptographic keys and thus compromise the whole sensor network. A specific sensor might be caught, and information stored on it might be obtained by an opponent.

5. False Node

A false node includes the addition of a node by an opponent and reasons the addition of malicious data. An invader might add a node to the method that feeds wrong data or stops the channel of correct data. Inclusion of malicious node is one of the most hazardous attacks that can happen. Malicious code injected in the network could extent to all nodes, possibly destroying the complete network.

B. *Passive Attacks*

The illegal invaders monitors and listens to the communication channel are known as passive attack. The Attacks against secrecy is inactive in nature.

1. Attacks against Secrecy

The main secrecy problem is not that sensor networks allow the collection of information. In point, much evidence from sensor networks could possibly be collected through straight location observation. Rather, sensor networks increase the privacy problem because they make large sizes of information simply available through distant contact. Hence, opponents need not be actually present to maintain observation. They can gather information at low-risk in unknown manner. The common attacks against sensor secrecy are:

2. Monitor and Snooping

This is the supreme common attack to secrecy. By snooping to the data, the opponent could simply notice the message contents.

3. Traffic Investigation

Even when the messages transported are encoded, it still leaves a high probability study of the message patterns. Sensor actions can possibly disclose sufficient information to allow an opponent to reason malicious destruction to the sensor network.

4. Mask Opponents

One can add their node or negotiate the nodes to hide in the sensor network. After that these nodes can duplicate as a regular node to appeal the packets, then misroute the packets, directing the privacy investigation.

II. LITERATURE SURVEY

Dr.G.Padmavathi et al.[1] explain about how the sensors are placed in aggressive environment and so they are more vulnerable to attacks. It also explains about different attacks on wireless sensor network and its security goals. Zhen Yu et al. [2] proposed a dynamic en-route quarantine scheme for filtering false data injection attacks and DoS attacks in wireless sensor networks. In this scheme, each node uses its own auth-keys to authenticate their reports and a legitimate report should be endorsed by nodes. The auth-keys of each node form a hash chain and are updated in each round. The cluster-head distributes the first auth-key of every node to forwarding nodes and then sends the reports followed by released auth-keys. The forwarding nodes verify the authenticity of the disclosed keys by hashing the distributed keys and then check the integrity and validity of the reports using the released keys. According to the confirmation results, they inform the next-hop nodes to either drop or keep on forwarding the reports. This method is repeated at every hop by each forwarding node.Arif Selcuk Uluagac et al.[3] This paper introduces energy-efficient Virtual Energy-Based Encryption and Keying (VEBEK) scheme for WSNs that significantly reduces the number of broadcasts needed for rekeying to avoid hard key. VEBEK is a secure communication structure where RC4 encryption mechanism is used to protect the data. Rongxing Lu et al.[4].This paper recommends a Bandwidth efficient co-operative authentication scheme which is more scalable and reliable and saves more energy by detecting and filtering the majority of injected false data with slight extra overheads at the en-route nodes. In this scheme CNR (co-operative neighborhood router) based authentication mechanism is used to filter data.

A. *En-route Filtering Techniques*

The objective of the en-route filtering technique is to enhance the effectiveness of the filtering which reduces the false data. Various techniques of en-route filtering are:

1. Dynamic En-route Filtering

In dynamic en-route filtering scheme, each node has a hash chain of authentication keys used to approve reports; meanwhile, a legitimate report is validated by a certain number of multiple message authentication codes generated by nodes. First, each node distributes its key to forwarding nodes. After sending reports, the sending nodes release their keys, allowing the forwarding nodes to verify their reports. The Hill Climbing key approach is used for disseminating of the keys and ensures that the nodes closer to clusters have stronger filtering capacity. In this approach**,** when an event is triggered inside cluster, the cluster-head is responsible for collecting the *sensing reports* from sensing nodes and aggregates them into the *aggregated reports*. Then the aggregated reports are forwarded to the base station through forwarding nodes. Thus each sensing report contains one MAC that is produced by a sensing node using its authentication key (called *auth-key* for short), while each aggregated report contains n distinct MACs, where n is the maximum number of compromised nodes allowed in each cluster as shown in fig.2.

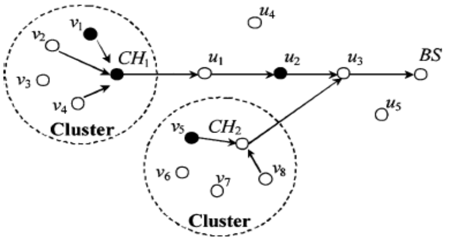


Fig2. Cluster of sensor nodes.[2]

2. VIRTUAL ENERGY BASED ENCRYPTION AND KEYING (VEBEK)

VEBEK is energy efficient virtual energy based encryption and keying scheme for WSNs that meaningfully reduces the number of broadcasts needed for rekeying to avoid hard keys. VEBEK is a secure communication framework where detected data is encrypted using a scheme based on a permutation code generated via the RC4 encryption mechanism. The key fed to the RC4 encryption mechanism dynamically changes as a task of the residual virtual energy of the sensor. Thus, a one-time dynamic key is engaged for one packet only and different keys are used for the consecutive packets of the stream. VEBEK is able to efficiently notice and filter false data which is inserted into the network. VEBEK framework consists of three modules: Virtual Energy-Based Keying Module, Crypto Module and Forwarding Module as shown in Fig3. The key generated by Virtual Energy Based Keying Module is dynamic in nature. A sensor node calculates keys based on its residual virtual energy of the sensor. This key is fed into the crypto module. The crypto module consists of RC4 code for simple encoding operation which basically is the process of permutation of the bits in the packet. Forwarding module handles the process of sending or receiving of encrypted packets along the path to the sink. The dynamic key which is produced by virtual keying is very important as it is makes very problematic for the invader to interrupt enough packets to break the encoding algorithm.

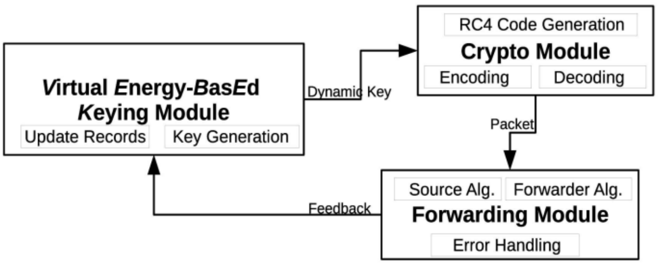


Fig3. VEBEK framework [3]

RC4 Encryption Mechanism

The packets in VEBEK contains ID (I-bits), type (T-bits) (assuming each node has a type identifier), and data (D-bits).

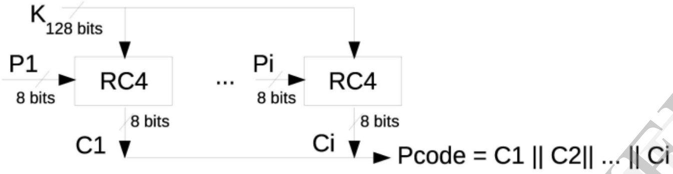
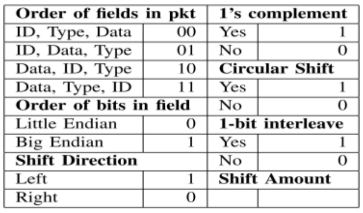


Fig4.RC4 encryption mechanism [3]

The permutation code P can be plotted to a set of actions to be taken on the data stream grouping. For example, the actions and their matching bit values can include simple operations such as shift, interleaving, taking the 1's complement. For example, if a node calculated the following permutation code P =1100100101, the string in Fig.5 (a) becomes the string in Fig.5(d) before it is transferred. The receiver will perform the same operations (since the inputs to RC4 are stored and updated on each sensor) to correctly decrypt the packet. To confirm correctness, the receiver matches the plaintext ID with the decrypted ID.



Order of fields in pkt		**1's complement**	
ID, Type, Data	00	Yes	1
ID, Data, Type	01	No	0
Data, ID, Type	10	**Circular Shift**	
Data, Type, ID	11	Yes	1
Order of bits in field		No	0
Little Endian	0	**1-bit interleave**	
Big Endian	1	Yes	1
Shift Direction		No	0
Left	1	**Shift Amount**	
Right	0		

Fig4.Encoding operation

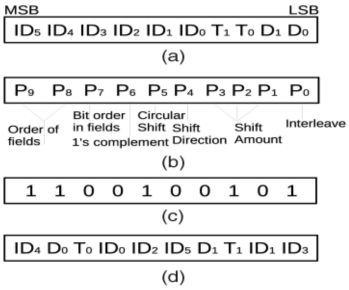


Fig5. A sample encoding operation [3]

3. BECAN

BECAN is bandwidth efficient co-operative authentication scheme for filtering false data**.** The proposed BECAN scheme can save energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. To filter the false data injected by compromised sensor nodes, the BECAN adopts Cooperative Neighbor Router (CNR)-based filtering mechanism.

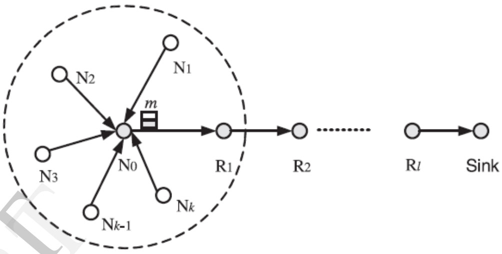


Fig6. Co-operative CNR based authentication mechanism [4]

In CNR created authentication mechanism, when a source node SN0 is complete to direct a report m to the sink via an established routing path SR_{N0}:[R_1-R_2-R_l-sink]it first supports to its K nearby nodes SN_{N0}:[N_1,N_2,….N_k] to co-operatively validate information MAC as shown in fig6. from SN_0USN_{N0} to the sink through routing R_{N0},where

$$\mathbf{MAC} = \begin{pmatrix} mac_{01} & \cdots & mac_{0l} & mac_{0s} \\ mac_{11} & \cdots & mac_{1l} & mac_{1s} \\ mac_{21} & \cdots & mac_{2l} & mac_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ mac_{k1} & \cdots & mac_{kl} & mac_{ks} \end{pmatrix},$$

Fig7.Message authentication codes

En-route filtering

When each sensor node SRi along the routing SR_{N0} receives (x,t,MAC) from its neighboring node, the integrity of the message x and the timestamp t are checked.If the timestamp t is out of date,the message (x,t,MAC) will be discarded else it has to invoke the algorithm of CNR based MAC verification. If the returned value is accept SRi will forward the message (x,t,MAC) to its next node, otherwise (x,t,MAC) will be discarded

Algorithm: CNR based MAC authentication

For each routing node $SR_{j\,,}$ where(j=0,1,……l), it uses the non-interactive key pair establishment to compute shared keys with each node in $\{SN_0,SN_1……..SN_k\}$ as $K_{0j},K_{1j}…….K_{kj}$

Procedure: CNR based MAC authentication

Input: K_{0j}, $K_{1j}…….K_{kj}$ x,t,MAC

```
1. Set return value=”ACCEPT”
2. For i=0 to k do
3. $mac_{ij}$=MAC (x ||t, $K_{ij}$, 1)
4. If $mac_{ij} \oplus$ macij≠0 then
5. Set return value=”REJECT”
6. End for
```

III. COMPARATIVE ANALYSIS

To compute the energy of SEF, the expression is given as

$$E= Lar(H+\beta*1/p) \tag{3.1}$$

Lar=length of the authenticated report with multiple macs

Lnr=length of the normal report

β= no. of false data

P=no. of probability the false data is filtered

H=no. of hops.

The energy consumption for transmitting normal report is

$e=Lnr*H\ (1+\beta)$

For authenticating report is

$E=Lar(H+\beta*1/P)$

In DEF, each forwarding node not only forwards report r, but also the messages K (n), K(t) and OK.So,

$Lar=Lnr+\gamma(Lk(t)+Lok)+\delta Lk(n)$

Where Lnr, Lk(n), Lk(t), Lok are length of the corresponding report and messages and γ and δ are the ratio of number of messages K(n),K(t) and OK
Suppose a normal report is 24 byte long, which means

Lnr=24*8=192 bits

In DEF,we assume each MAC and each secret key are both 64 bit long and OK message and each index including node index and key index are 8 bits long. Now if the values are l = 2, t = 5, v = w = 20 and n = 10. Therefore, we can derive that
L_R = 24× 8 + t × (8 + 8 + 64) = 592 bits,
$L_{K(t)}$ = t × [8 + 8 + (l + 1) × (8 + 64)] = 1160 bits
$L_{K(n)}$ =n/t*$L_{K(t)}$=2320 bits
L_{OK} = 8 bits,
Lar=732 bits
Now for SEF p=0.05 since the number of false data filtered is less i.e. Lar=306 bits, where a key index is 10-bit long and the Bloom filter is 64-bit long as set in SEF.So $E_{sef=}$306(H+10/0.05) (as there are no control messages) (from equation 1) =306(H+200)
Now for DEF
Lr’=732 and p=0.275
So, E_{def} = 732(H+10/0.275) (from equation 1)
= 732(H+36)
So compared with SEF, DEF can save 1- E_{DEF}/E_{SEF} that is approximately 50% of energy is saved.

Table 1: Comparative analysis of the En-route filtering techniques

Technique	Parameters	
	False data filtering with hops	Energy efficiency
Dynamic En-route filtering	90% of false data is dropped within 10 hops	50% of energy saved
VEBEK	90% of false data is dropped within 15 hops	60-100% of energy saved
BECAN	90% of false data is dropped within 15 hops	80% of energy saved

IV. CONCLUSION

The DEF saves more energy compared to SEF if you consider removal of the false data from WSN.VEBEK requires less energy compared to DEF and SEF for the transmission of data.BECAN saves more energy compared to SEF if you consider removal of the false data from WSN.DEF consumes more energy while it remove false data in less number of hops BECAN and VEBEK consumes less energy while it requires more number of hops to filter false data. Whether concern is energy consumption or security, we can either select DEF or BECAN/VEBEK for removing false data from WSN.

REFERENCES

[1] Dr. G.Padmavathi, Mrs. D.Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[2] Zhen Yu, Member, IEEE, and Yong Guan, Member, IEEE, “A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks”, IEEE/ACM TRANSACTION ON NETWORKING, VOL. 18, NO. 1, FEBRUARY 2010.

[3] Arif Selcuk Uluagac,Raheem A. Beyah, Yingshu Li, John A.Copeland,” Virtual Energy-Based Encryption an Keying for Wireless Sensor Networks,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010.

[4] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, Xuemin (Sherman) Shen, “A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks”, IEEE TRANSACTIONSON PARALLEL ANDDISTRIBUTED SYSTEMS, VOL. 23, NO. 1, JANUARY2012

[5] Syama M,Deepti C,” An Evaluation Of En-Route Filtering Methods For False Data Injection Attack In WSNs” International Journal of Engineering Research & Technology.