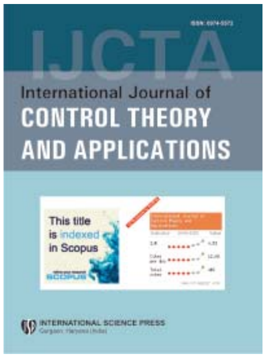

International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 10 • Number 27 • 2017

DoS Attacks Detection in Clustered Wireless Sensor Networks using Signature based Authentication

Jerine.S[a] and Julia Punitha Malar Dhas[b]

[a]*Research Scholar, Department of Computer Applications, Noorul Islam University, Kumaracoil, Thuckalay, K.K.Dist-629180, TamilNadu, India.*

E-Mail: ssjerine@gmail.com

[b]*Professor and Head, Dept of Computer Science and Engg, Noorul Islam University, Kumaracoil, Thuckalay, K.K.Dist-629180, TamilNadu, India.*

E-Mail: julaps113@yahoo.com

Abstract: Wireless Sensor Network (WSN) contains small sensor nodes with limited computational and communication capabilities. It is mainly used to observe the physical or environmental conditions such as temperature, noise, vibration, pressure and so on. Due to the scattered deployment of sensor nodes, it is vulnerable to many types of attack such as wormholes, selective forwarding and Sybil attacks. In such a network, authentication is important for secure data transmission also to identify wrong access requests from unauthorized users. We propose an authentication mechanism to detect DoS attacks based on signatures. Our method authenticates the source node and detects DoS attack by identifying malicious data using signatures. The proposed methodology can save sensor node's energy by early detecting the majority of malicious data with less overhead by the cluster heads. In addition, only a very small number of injected malicious data needs to be checked by the sink, which thus diminishes the trouble of the base station. Performance evaluation demonstrates the efficiency of the proposed scheme in terms of high detection rate and less transmission delay.

Keywords: *Wireless Sensor Network, DoS attack, Signature, Authentication, Filtering malicious data.*

1. INTRODUCTION

A Clustered Wireless Sensor Network is composed of large number of sensor nodes, Cluster Head, Routing nodes and a special sink node. These nodes are interconnected to attain distributed sensing tasks. Each sensor node is low cost but has required sensing processing and communicating components. Therefore messages sent by the sensor node will be reported to base station via the cluster head [1] [2].

Wireless Sensor Networks are typically set up in unattended environments. Therefore they are susceptible to many types of attacks such as selective forwarding, wormholes and Sybil attacks [3][4]. It may also be affected by false data attack [5]. An opponent first compromises the sensor node for inserting false data, and uses them to send bogus messages to the sink node which causes high level error decision and energy wastage in the routing nodes. It is not easy to identify the injected false data accurately in wireless sensor networks. Simultaneous broadcasting of false data to the sink node not only causes energy wastage but also requires deep verification functions. Therefore injecting false data should be executed in both routing nodes and in sink node. For this many false data filtering mechanisms were developed [6][7][8]. Most of the existing mechanisms use symmetric key cryptography. According to this once the attacker hacked the secret key then the reliability of the filtering mechanism will be degraded.

In this paper we propose a signature based authentication scheme for identifying DoS attacks by filtering malicious data in wireless sensor networks. When comparing with the previous schemes the proposed scheme provides high filtering probability and high reliability.

The rest of the paper is organized as follows. Section 2, reviews some related works. Section 3, introduces the system model and design goal. Section 4, presents the proposed methodology. Section 5, analyzes the results and performance, and finally section 6 concludes the paper.

2. RELATED WORK

In the recent years many research works were developed for filtering the injected malicious data attack n wireless sensor network. In [1], a new bandwidth efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. It uses TinyECC based non interactive key pair establishment and message authentication code. Two designs used in this are nodes initialization and deployment and sensed results reporting. This method saves energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink which largely reduces the burden of the sink. In [3], Ren et al. propose a more efficient location aware end to end data security design (LEDS) to provide end to end security including false data filtering capability. In [5], Zhu et al. present an interleaved hop by hop authentication (IHA) for filtering false data. In IHA each node is associated with two other nodes along the path, one is the lower authentication node and other is the upper authentication node. An en-route node will forward the data if it is successfully verified by its lower authentication node. In [8], Ye et al. designed a filtering algorithm called SEF. In this each sensed data is certified by compound keyed message authentication code (MAC). It uses random subset of keys to verify the MAC. Also to save bandwidth it uses bloom filter. In [9], Yang et al. proposed a Location Based Resilient Secrecy (LBRS), which adopts location key binding mechanisms to reduce the damage caused by node compromise and further mitigate false data generation in wireless sensor networks. In [10], Zhang et al. provide a public key based solution to en route filtering. It uses private keys to bind the location based keys. In [11], Anjali et al. proposed a scheme based on ID based signatures for efficient group verification of multiple signatures to mitigate gang injection of false attack threat. It allows any pair of users to communicate securely and to verify each other’s signatures without exchanging public key certificates. In [12], Vimala et al. proposed a cooperative authentication scheme to sort out the false data injection by set of adversary. Virtual Backbone Scheduling (VBS) scheme saves energy of sensor nodes by turn off their radios having low energy. In [13], Uma et al. proposed CAFS: an authentication scheme for filtering false data, CNR based MAC code technique is used in this paper saves energy by early detecting and filtering the majority false data with less overhead. In [14], Xinxin et al. proposed a fast signature verification scheme with attractive characteristics such as powerful security resilience, good scalability, and immediate authentication. In [15], Bellare et al. proposed an identity based pairing free signature scheme with reduced signature size.

3. SYSTEM MODEL

This section formulates the network model, security model and identifies the design goal.

3.1. Network Model

We consider a clustered wireless sensor network. It consists of an amount of sensor nodes SN = {SN_0, SN_1, ...}, they are deployed arbitrarily in the area A, Cluster Heads (CH), and a base station (BST). The powerful node used for data collection computation and storage is the base station and is liable for initializing the sensor nodes. A unique identifier is given to all sensor nodes for identification purpose. Communication is bidirectional ie, sensor nodes inside the communication range may communicate with each other. Sensor nodes can forward data via established route through the cluster heads. So such undirected graph G = {V, E} is used to model such type of wireless sensor networks, where V = {V_1 ,V_2 ,.........} is the set of sensors SN = {SN_0, SN_1.........} and E = {(V*i*,V*j*) | V*i*,V*j* € V}is the set of edges. Distance between two sensor nodes V*i*,V*j* is measured by *d*(V*i*, V*j*). An edge e_{ij} indicates whether there exists a communication link between nodes V*i* and V*j* or not is defined as,

$$e_{ij} \quad = \quad \begin{cases} 1, d(\mathrm{V}i, \mathrm{V}j) \le \mathrm{R} \\ 0, d(\mathrm{V}i, \mathrm{V}j) > \mathrm{R} \end{cases}$$

3.2. Security Model

If a wireless sensor network is unprotected, malicious adversaries may launch security attacks to degrade the network functionalities. Attackers can send malicious data that floods into the sink then the sink will be surely affected by DoS attack. Therefore our model focuses on detecting the false data injected by malicious node.

3.3. Design Goal

The design is to develop an efficient signature based authentication scheme for identifying the malicious data injected in the wireless sensor networks.

4. PROPOSED SCHEME

We propose an authentication scheme to filter malicious data that were injected by compromised nodes in clustered wireless sensor networks. This scheme uses signatures to provide data confidentiality. It uses cluster head nodes to ensure efficient filtering of malicious data.

Each sensor node in the cluster is preloaded with a master key and each sensor is mutually authenticated by its cluster head (CH). Before forwarding the sensed data, it is authenticated by the cluster head node. For that a secret key domain {K1, K2…..} is created by cluster head (CH) and distributed to all cluster members. The signature generated by the sensor node is forwarded to base station via cluster head is shown in Fig 1. The base station also verifies the received signature to identify the malicious data.

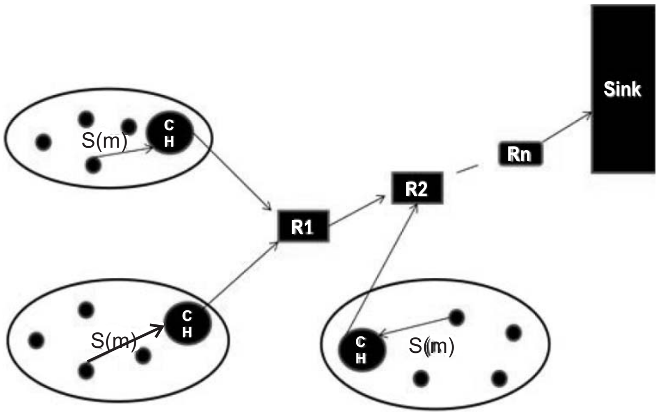

Figure 1: Signature based authentication

The proposed methodology includes three phases: Node initialization and key distribution, Signature generation, and Signature verification.

4.1. Node Initialization and key distribution

Each sensor node is initially set up with an identifier and a master key because sensor nodes are usually installed in unattended terrains. Base station invokes algorithm 1 for initializing the sensor nodes. After each sensor node is initialized it is mutually authenticated by cluster head, which generates a key domain for its members. Using this key domain sensor node can make communication with its neighbors in the transmission range.

Algorithm 1. Node Initialization and Key Establishment

```
Input: {id, master key}, SN = {SN0, SN1, …}
Output : Secret key domain Ki = {K0, K1 ….}.
1.  For each node SNi€N do
        Preload SNi with id and master key
2.  Mutually authenticate SNi by CH
3.  Generate secret key domain(Ki)
4.  End for
5.  Return secret key domain (Ki)
```

4.2. Signature Generation

When a sensor node SNi is ready to transmit message (Mi), it first compute the signature and attaches current timestamp (T) and identifier (IDi) and is forwarded through SNi → CH → BST. Algorithm 2 is used for generating signature.

Algorithm 2. Signature Generation

```
Input : SN, mi, Ti, IDi, Ki, KRi
Output : Signature
1.  SNi computes hash code of message mi called H = H(m).
2.  Encrypt H using secret key Ki called EH = EKi(H(m))
3.  Encrypt EH using private key KRi called Signature = EKRi(EKi(H(m))).
4.  Return Signature
```

4.3. Signature Verification

The generated signature together with timestamp and identifier of source node <signature, Ti, IDi> is then forwarded through Cluster Head. When a cluster head CH$_i$ receives signature it invokes Algorithm 3 for verification. If the algorithm returns "true" then it forwards the message to base station otherwise it discards the message.

Algorithm 3. Signature Verification

```
Input : Signature,  Ti, IDi, KPi, Ki
Output: true or false
1.  Set returnvalue = "True"
2.  Calculate Tj.
```

```
If $(T_i – T_j) >= \Delta T$
Discard the message
Else
Decrypt the signature using sender’s public key $KU_i$ will results encrypted hash code.
Decrypt the encrypted hash code using secret key $K_i$ will results hash code.
Compute the hash code $H(m)^{\sim}$
If $H(m)$ XOR $H(m)^{\sim} \neq 0$
Set return value = “False”
Break
Return returnvalue
```

5. PERFORMANCE EVALUATION

The performance of proposed methodology is evaluated using malicious data detection rate and transmission delay.

5.1. Detection rate

$$\text{Detection rate} = \text{Number of packets accepted / Total number of packets.}$$

Figure 2 illustrates the detection rate of proposed scheme. The proposed scheme uses signature authentication to identify the injected malicious data in wireless sensor network. It uses cluster heads to verify the data before it s transmitted to base station, thus malicious data can be identified as early as possible.

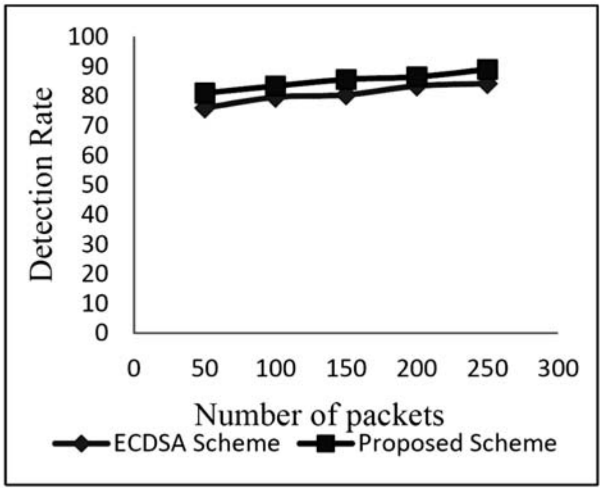

Figure 2: Detection Rate

5.2. Transmission delay

$$\text{Delay} = \text{(Arrival time – sending time)}$$

The existing ECDSA scheme has high transmission delay because of complex and broadcast authentication function. But the proposed scheme in this paper uses simple authentication functions which needs less verification requirements thus automatically reduces transmission delay is shown in Figure 3.

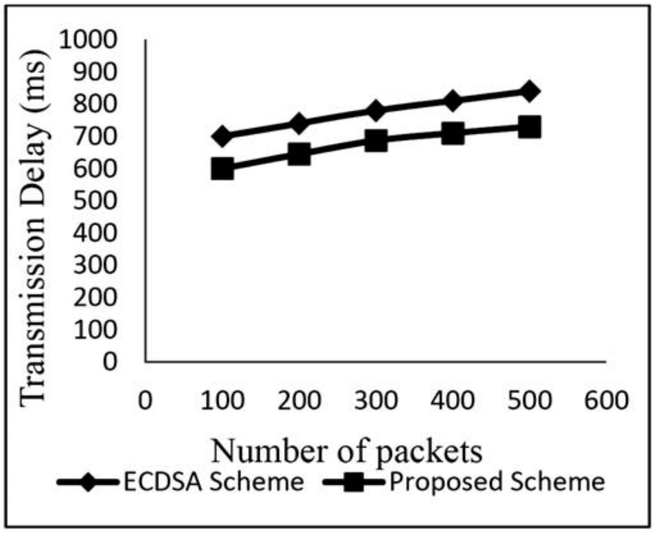

Figure 3: Transmission Delay

6. CONCLUSION

Due to the bounded capability of a Sensor node, it is difficult to prevent the sensor nodes from DoS attack. DoS detection mechanism used in wireless networks are not suitable for Wireless Sensor Network because of limited energy and lack of management. The proposed signature based authentication methodology in this paper detects DoS attack by filtering injected malicious data in wireless sensor networks. Performance study shows that the proposed scheme provides high reliable data transmission, good scalability and immediate message authentication using signatures. Due to simple and energy efficiency this scheme is well suits to wireless sensor networks.

REFERENCES

[1] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, Xuemin Shen,"BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Filtering injected false data in wireless sensor networks",IEEE Computer Society, 2012.

[2] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," Ad Hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.

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

[4] V.C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 8, no. 1, pp. 1-24, Jan. 2008.

[5] 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," Proc. IEEE Symp. Security and Privacy, 2004.

[6] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[7] Z. Zhu, Q. Tan, and P. Zhu, "An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network," Proc. 10th Asia-Pacific Network Operations and Management Symp.(APNOMS '07), pp. 457-465, 2007.

[8] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04, Mar. 2004.

[9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), pp. 34-45, 2005.

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang,"Location-Based Compromise-tolerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 247-260, Feb. 2006.

[11] Anjali Thampi, Nithya," An efficient ID based scheme for filtering gang injected false data in wireless sensor networks", IJARCCE, Vol 2, ISSN:2319-5940, 2013.

[12] D.Vmala, Srinivasan, Vinoth, Arun Prasath," Protection of wireless sensor network from gang injected false data attack", IJAREEIE, Vol 1, ISSN:2320-3765, 2014.

[13] Uma Narayan, Arun Soman, "CAFS: Cluster based authentication scheme for filtering false data in wireless sensor networks", IJARCCE, ISSN: 2319-5940, 2013.

[14] Xnxin Fan, Guang Gong, "Accelerating signature dased broadcast authentication for wireless sensor networks", Elsevier, 2011.

[15] M.Bellare, C.Namprempre, G.Neven," Security proofs for identity based identification and signature schemes", Springer 2004.