An enhanced wormhole detection approach for hop by hop message authentication

[1]J. Jasmine jose, [2]B.Prasath

[1]*Student,* [2]*Assistant Professor Dept of Computer Science and Engineering, CSI College of Engineering, Nilgiris - 643 215*, India
[1] jasminecsiooty@gmail.com, [2]prasathcsi@gmail.com

Abstract

Objective: To provide Message authentication and detect the wormhole attacks in the wireless sensor networks.
Methods: Source anonymous message authentication (SAMA) scheme is used for Hop-by-Hop Message Authentication. In Hop-by-Hop Message Authentication process each nodes in the routing path is confirm the authentication and integrity of the messages. A wormhole attack causes several damages while routing. Here the system introduces Enhanced Wormhole attack Detection (EWAD) based on per hop latency which is used for detect the wormhole attack. Per Hop latency is calculated based on round trip time (RTT) while route discovery phase.
Results: In this experimental analysis, the performance of proposed system is highly efficient in terms of energy consumption, end to end delay.
Conclusion: The system offers an efficient hop-by-hop message authentication mechanism for WSNs without any threshold limitation. Wormhole attack is one of routing attack that can be occurred during routing process. To detect that attacks Per Hop latency is computed based on round trip time (RTT).According to that value wormhole attack can be detected.

Keyword: Message Authentication, Wireless Sensor Networks, Round trip time, Hop latency.

1. Introduction

Wireless sensor networks can be utilised by various mission-critical purposes such as target tracking in battlefields and emergency response. In this application, reliable and timely delivery of sensory data plays a critical role for the achievement of the mission [1].

Information gathering is one of most significant functions presented by WSNs, where sensor Information has to be collected from sensor nodes to one or few data grouping sites (sinks) [2].

Each node of the network considers three subsystems. There are sensor subsystems, processing subsystem, communication subsystem. The sensor subsystem performs the sensing operation such as environmental conditions, the processing subsystem performs local computation on the sensed data and the communication subsystem performs exchanging the information among nodes .The each sensor have partial sensing area, less power for system processing and energy consumption, networking a huge numbers of sensors gives efficient robustness, reliable, and accurate sensor network covering a wider region [3].

1.1. Applications of wireless sensor networks

Area monitoring is main applications of wireless sensor networks.
The Environmental Sensor Networks has evolved to cover various appliances of WSNs. This takes account of sensing volcanoes, oceans, glaciers, forests, etc [4].
Observing the gas levels at danger area needs the usage of high-end, sophisticated equipment, capable to assure industrial policies [5]. Wireless internal monitoring system assists to keep tabs on large areas as well as ensures the precise gas concentration degree.
An air quality monitoring system wants the use of precise wireless sensors, rain & wind resistant solutions and reaping techniques to assure extensive liberty to machine that will likely have tough access.

1.2. Literature survey

The system introduced for clear the attacks, which call a false data injection attack. To check the validity of report the system facilitates the base station. The report has received number of nodes does not greater than the certain threshold. The system wants to remove the false data packets before reach the destination. Secure Information Aggregation (SIA) method overcome the issues of false data injection using statistical techniques and interactive proofs; guarantee that finally the results can be combined by aggregation node. This system is utilized by large-scale sensor networks where the sensor node reports want to be relayed over several hops before it reaches the base station [6] [7].

Wormhole assist a number of attacks against key organization and routing protocols [8,9]. If wormhole attacker directs the link, they cause many damages to the network. That attack can be damage the data aggregation, routing, clustering protocols and security of the systems. This attack can be introduced without any access to the cryptographic keys or compromising any genuine node in the network. The wormhole attack is predominantly dangerous attack. The packet transmission is done by considering the intermediate transmission range.

The system proposed an efficient source anonymous message authentication (SAMA) technique that is based on the optimal modified ElGamal signature (MES) method on elliptic curves. The MES technique is secure message attacks and adaptive chosen-message attack in the arbitrary oracle representation. This method enables the every node to authenticate the message so that all tainted packets can be dropped to conserve sensor power. Main contribution of the system is (i) a source anonymous message authentication (SAMA) method can give unconditional source anonymity; (ii) an efficient hop-by-hop message authentication technique is generated without any threshold limitation; (iii) the network execution criteria is devised on source node privacy protection in WSNs [10].

2. Proposed source anonymous message authentication on elliptic curves

The system proposed is an unconditionally secure and well-organized SAMA. Every message m to be released, the message sender, or the sending node, produces a source anonymous message authenticator for the message m .The creation is based on the MES scheme on elliptic curves.

2.1. MES scheme on elliptic curves

Let p > 3 is an odd prime. An elliptic curve is represented by an equation

$$E: y^2 = x^3 + ax + b \; mod \; p,$$

Where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \not\equiv 0 \; mod \; p$

E- Elliptic curve

G= $(\mathrm{x_G}, \mathrm{y_G})$ is a base point on E($\mathrm{F_p}$) .Order of this is huge value N. $d_A \in [1, N-1]$ is a private key. That can be randomly selected by a user A. Then, user compute public key Q_A from$Q_A = d_A \times G$.

2.2. Signature generation algorithm

Sender to sign the message, it follows below steps

1. choose a random integer $k_A, 1 \leq k_A \leq N - 1$.
2. Compute $r = x_A \; mod \; N$,
   $(x_A, y_A) = k_A G$. If r= 0, go to step 1.
3. determine $h_A \overset{l}{\leftarrow} h(m, r)$
   h - Cryptographic hash function
4. compute $s = r d_A h_A + k_A \; mod \; N$.
   If s=0 go to step 2.
5. Finally signature is the pair (r, s).

2.3. Signature verification algorithm

The receiver to authenticate sender signature, they should have a copy of sender public key Q_A.The receiver authenticate sender (Alice's) signature; they should have copy of her public key Q_A .

1. Verify that $Q_A \neq \mathcal{O}$ otherwise invalid
2. Verify that Q_A lies on the curve
3. Verify that $nQ_A = \mathcal{O}$

// O - special point

To verify the signature, receiver follows these steps

1. Check r and s are integers in $[1, N-1]$. If not, the sign is unacceptable.
2. determine $h_A \overset{l}{\leftarrow} h(m, r)$
   h- Same as Signature generation hash function
3. Compute $(x_1, x_2) = sG - rh_A Q_A \ mod\ N$.
4. The signature is suitable if $= x_1\ mod\ N$, unacceptable otherwise.

The signature is properly generated, then:

$(x_1, x_2) = sG - rh_A Q_A$

$= (rd_A h_A + k_A)G - rh_A Q_A$

$= k_A G + rh_A Q_A - rh_A Q_A$

$(x_1, x_2) = k_A$G

$They\ have\ x_1 = r$ and the signature is accepted by a verifier.

2.4. Proposed SAMA on elliptic curves

2.4.1 Authentication generation algorithm

Suppose m is a message to be transmitted. $\mathrm{d_t}$ is a private key of the message sender , ranging from $1 \leq \mathrm{t} \leq$ N.To compute an efficient SAMA for message m, the sender follow execute the three steps:

To compute effective SAMA for message, sender execute the below steps:

1. Choose an arbitrary and pair wise various k_i for each $1 \leq i \leq n-1, i \neq t$ and calculate r_i from$(r_i, y_i) = k_i G$.
2. Select a random $k_i \in \mathbb{Z}_p$ and calculate r_t from $(r_t, y_t) = k_t G - \sum_{i \neq t} r_i\, h_i Q_i$ such that $r_t \neq 0$ and $r_t \neq r_i$ for any $i \neq t$ where$h_i \overset{l}{\leftarrow} h(m, r_i)$.
3. calculate $s = k_t + \sum_{i \neq t} k_i + r_t d_t h_t \ mod\ N$.

The SAMA message is define as:

$\mathcal{S}(m) = (m, \mathcal{S}, r_1, y_1, \ldots r_n, y_n, s)$.

2.5. Verification process

Verification algorithm: For message receiver to verify an alleged SAMA $(m, \mathcal{S}, r_1, y_1, \ldots r_n, y_n, s)$ they must have a copy of the public keys$Q_1, \ldots Q_n$. Then he,

1. Verify that $Q_i \neq \mathcal{O}, i = 1, .. n$ otherwise unacceptable.
2. Verify that $Q_i, i = 1, .. n$ lies on the curve
3. Verify that $nQ_i = \mathcal{O}, \mathrm{i} = 1, .. \mathrm{n}$

Later than that, receiver follows below steps:

1. Check $r_i, y_i, i = 1, .. n$ and s are integers in $[1, N-1]$. If not, the signature is unacceptable.
2. Compute $h_i \overset{l}{\leftarrow} h(m, r_i)$
   h is same as signature generation hash function
3. Compute$(x_0, y_0) = sG - \sum_{i=1}^{n} r_i\, h_i Q_i$.
4. The signature is acceptable if the first coordinate of $\sum_i (r_i\,, y_i)$ equals $x_{0,}$ otherwise unacceptable.

In fact, if the SAMA has been properly created without any modification then calculate:

$$(x_0, y_0) = sG - \sum_{i=1}^{n} r_i\, h_i Q_i$$

$$= \left(k_t + \sum_{i \neq t} k_i + r_d d_t h_t\right) G - \sum_{i} r_i h_i\, Q_i$$

$$= \sum_{i \neq t} k_i\, G + (k_t G - \sum_{i \neq t} r_i\, h_i Q_i)$$

$$= \sum_{i \neq t} (r_i\,, y_i) + (r_t, y_t)$$

$$(x_0, y_0) == \textstyle\sum_i (r_i, y_i)$$

Therefore, the verifier always accepts the SAMA.

2.6. Enhanced wormhole attack detection (EWAD) based on per hop latency

Wormhole attack is one of the routing attacks. It can be causes several damage to the route discovery process or routing process. In wormhole attack, the malicious nodes will tunnel the eavesdrop packets to a remote position in the network and retransmit them to generate fake neighbour connections, thus damage the network and weakening some security enhancements.

The system introduces a round trip time (RTT) and neighboring node based wormhole attack detection approach. Per Hop latency is computed based on round trip time (RTT) which can be executed for all the links among source and destination nodes during the route discovery process. RTT is referred as the time difference between RREQ and RREP packet propagation at a node.

RTT = RREPTS – RREQTS– RTT previous

RREQ TS: Timestamp when the RREQ packet is broadcasted by the current node X.

RREPTS: Timestamp when the RREP packet is received by the current node X.

RTT previous: RTT value of the previous hop.

The link with maximum RTT per hop latency that exceeding threshold value would be represented as wormhole link and the corresponding nodes as suspicious wormhole peers.

3. Performance analysis

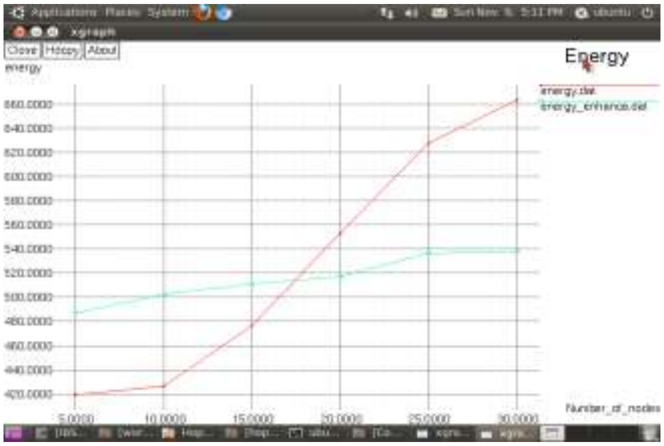
In this experimental analysis, the performance of the existing and the proposed system is compared. The existing system was SAMA based hop-by-hop message authentication technique and proposed system is Hop latency based Wormhole attacks detection Approach**.**The parameters like energy consumption, end to end delay are evaluated for comparison of the existing and the proposed system**.**

3.1. Energy consumption

Energy consumption is referred as the amount of energy taken for the processing and transmission of packets.

Figure 1. Shows that the when the number of node increases, the amount of energy consumed is less in the proposed system when compared to the existing system**.**

Figure 1.Energy consumption

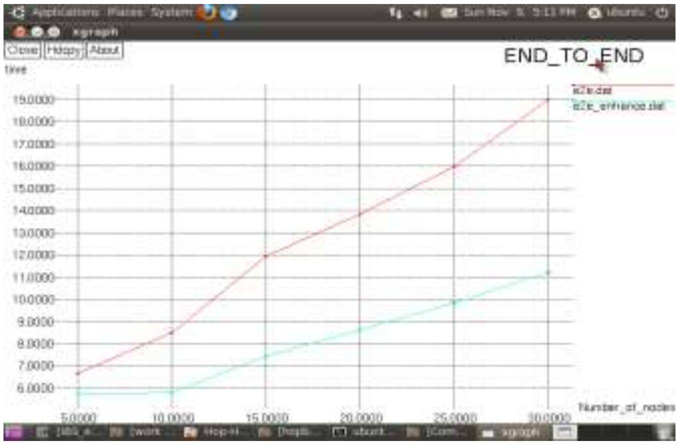


3.2. End to end delay

End-to-end delay is referred as the time taken for a packet to be transmitted across a network from source to destination.

Figure 2. shows that if the number of nodes is increases the end to end delay of the network is increased. The time taken for a packet to be transmitted across a network from source to destination is efficient compare to existing one.

Figure 2. End to end delay



4. Conclusion

In this system, a novel and efficient SAMA is proposed based on ECC. Assure the message sender privacy, SAMA method can be applied to any message to provide message authentication. The wormhole attack is introduced many damage during routing process. The system introduces a new wormhole attack detection method called Enhanced Wormhole attack Detection (EWAD) based on per hop latency. Per Hop latency computed based on round trip time (RTT) which is executed for all the links between source and destination nodes during the route discovery phase. The link with maximum RTT (Round trip time is exceeding the threshold value) which is marked as wormhole link and the consequent nodes as suspicious wormhole peers.

5. Reference

1. Lee, Eylem Ekici. MMSPEED: Multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. *IEEE Transactions on Mobile Computing*. 2006; 5(6), 738-754.
2. Haifeng Zheng, Feng Yang, Xiaohua Tian. Data gathering with compressive sensing in wireless sensor networks: A random walk based approach. *IEEE Transactions on Parallel and Distributed Systems*. 2015; 26 (1), 35-44
3. Shweta Bhatele, Lalita Bargadiya. Evaluation of communication overhead and energy consumption in wireless sensor network using different clustering techniques. *International Journal of software & Hardware Researching in Engineering*. 2014; 2(1), 81-87.
4. Yan-Xiao Li, Hao-Shan Shi, Shui-Ping Zhang. An efficient energy aware MAC protocol for wireless sensor network. International Conference ICMULT. *IEEE*. 2010; 1-4.
5. S. Tilak, Nael B. Abu-Ghazaleh, Wendi Heinzelman. A taxonomy of wireless micro sensor network models. *ACM Mobile Computing and Communications Review* (MC2R). 2002; 6 (2), 28-36.
6. F. Ye, H. Lou, S. Lu, L. Zhang. Statistical en-route filtering of injected false data in sensor networks. *IEEE*. 2005; 4, 839-850.
7. S. Zhu, S. Setia, S. Jajodia, P. Ning. An interleaved hop-by- hop authentication scheme for filtering false data in sensor networks. *Proceedings IEEE Symposium*. 2004; 259-271.
8. Y. Hu, A. Perring, D.B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. *Proceedings of 22nd Annual Conference of the IEEE Computer and Communication Societies*. 2003; 3, 1976-1986.
9. I. Khalil, S. Bagchi, N.B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. *IEEE Proceeding of International Conference on Dependable Systems and Networks (DSN 2005)*. Yokohama, Japan. 2005; 612-621
10. Jian Li, Yun Li, Jian Ren, Jie Wu, Fellow. Hop-by-hop message authentication and source privacy in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*. 2014; 25 (5), 1223-1232.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Citation:

J. Jasmine jose, B.Prasath. An enhanced wormhole detection approach for hop by hop message authentication. *Indian Journal of Innovations and Developments.* 2014; 3 (4), 74-79