Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 03, pp.13258-13264, March, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCHARTICLE

INCREASING DoS ATTACKS TOLERANCE FOR BROADCAST AUTHENTICATION IN WIRELESS SENSOR NETWORKS

***Ahmed Alghamdi and Mohammed Arozullah**

Department of Electrical and Computer Engineering, School of Engineering, Catholic University of America

ARTICLE INFO

Article History:
Received 07th December, 2014
Received in revised form
18th January, 2015
Accepted 07th February, 2015
Published online 17th March, 2015

Key words:

Security,
Wireless Sensor Node,
Denial of Service,
Broadcast Authentication,
DoS attack.

ABSTRACT

Broadcast authentication is one of the most fundamental services in Wireless Sensor Network (WSNs) that is being used to secure the application from different attacks like passive and active attacks, diverse layer attacks, cryptographic attacks and Denial of service (DoS) attacks. Security has become the most forefronts of network management and implementation. Digital Signature (DS) and Timed Efficient Stream Loss-tolerant Authentication (TESLA) are used in Wireless Sensor Networks to provide broadcast authentication, but still both are vulnerable to DoS attacks, attackers keep on broadcasting forged messages which will cause extra cost on the network due to power consumption. This will drain the nodes' energy, which will eventually reduce the network lifetime.In this paper we present approaches that are trying to defend against or contain such DoS attacks. We propose new scheme in receiver sensor node to recognize the forged message before authenticating the broadcast message to avoid the many unnecessary operations and to conserve the node's energy. The new proposed scheme uses a dynamic window (Wang *et al*., 2007) on the receiver side and reduces the DoS attacks to affect only a small part of the network. In this way we can reduce the energy consumption in order to increase the network lifetime and minimize the delay of broadcast messages.

INTRODUCTION

Problem Definition

As a result of the growth of networks over the years, the network attacking tools and methods have greatly improved. In 1980's the attackers needed to have a sophisticated level of computer programming and networking knowledge. Nowadays the attackers' methods and tools have improved drastically. The attackers are no longer in need of such sophisticated level of knowledge. Wireless Sensor Network is currently used in many variant applications; for example military, medical, navy, emergency and even civilian applications. In these networks, the sensors are actually restricted by resource constraints, regarding power consumption, transmission rate, available bandwidth and computational power.

State of The Art

The actual communication approach used in Wireless Sensor Network is broadcasting requests or commands from the base station to the sensor node; after that, the sensor nodes need to respond to those requests. Hence, the broadcast request needs to authenticate properly whether the requests are originally sent from the base station by using broadcast authentication to ensure the authenticity of messages. All the properties are satisfying the authentication property to provide a proof of the base station identity. Digital signature (Stallings, 2014 and Rivest *et al*., 1978) and TESLA (Perrig *et al*., 2000) are most the important well-known approach. Initially, the digital signature that is based on public key cryptography is considered impractical due to the high computational power needed to perform it with the constraints on resources in Wireless Sensor Network. However, recent studies have used modern devices to perform public key cryptography with more optimized digital signature techniques that is possible to perform PKC on resource-limited sensors.

The verification of Elliptical Curve Digital Signature Algorithm using 160-bit elliptical curve on AT Mega 128 processor will take 1.62 seconds (Gura *et al*., 2004). TESLA is classified as a symmetry approach; it provides asymmetry property by delaying the disclosure of authentication keys by using the uniqueness of key per time interval. Both Digital signature and Timed Efficient Stream Loss tolerant Authentication are vulnerable to DoS attacks. Since an attacker can inject a forged message forcing the sensors to do some unnecessary verification. This will result in spreading the forged message across the entire network, leading sensors to perform large computation and eventually draining the battery

****Corresponding author: Ahmed Alghamdi,***
Department of Electrical and Computer Engineering, School of Engineering, Catholic University of America.

power of sensor nodes (Wood and Stankovic, 2002 and Raymond and Midkiff, 2008).

Purpose

Many approaches were proposed to reduce unnecessary verification to secure broadcast authentication and forwarding of broadcast message. In this paper, we propose a new conducive system that compromises containment and prevention to increase DoS resistance as much as possible. This can be done by using a dynamic window. Simply this process will improve the performance of network and will reduce the damages of DoS attacks to only a small portion. In this way we can minimize energy consumption in the network and reduce the delay of broadcast. In section 2 we can review previous work related preventing DoS attacks against broadcast authentication. Then we illustrate the overall system in section 3. Section 4 will demonstrate the dynamic window scheme against the DoS attack in broadcast authentication. Section 5 contains security analysis and computation evaluation of the updated version of dynamic scheme. Section 6 will describes the simulation results and discussion regarding broadcast authentication against the DoS in wireless sensor network. Finally section 7 contains a conclusion to this paper.

Scope

The proposed scheme will detect the forged message and reduce the unnecessary computation in broadcast authentication. In this way we can easily reduce the injection of fake message in wireless sensor network by attackers as well as minimize the average broadcast delay.

Goals

To reduce the energy consumption and increase the wireless sensor network life time by doing proper broadcast authentication and verification against the forged message. This scheme had provided the improvement in energy efficiency, throughput and delay.

Hardware Configuration

- Processor: Any processor 500 MHZ and above.
- RAM: 1 GB and above.
- Hard Disk Space: 10 GB and above.
- Input Device: Network Interface Card, Standard keyboard and Mouse.
- Output Device: High resolution monitor.

Software Configuration

1. Operating System: Ubuntu 12.04.2
2. Tools: NS2

Related Work

In Wireless Sensor Networks, many solutions have been proposed to contain or resist Denial of service DoS attacks against broadcast authentication to prevent unnecessary authentication and verification which leads to more battery consumption. They may differ in assumption and purposes, regarding many criteria. Since this can be distinguished as a hop-by-hop schemes such as proposed in (Dong*et al*., 2008; Du *et al*., 2008; Huang *et al*., 2008) and not famed as hop-by-hop in (Ning *et al*., 2008). In wireless sensor networks, the hop-by-hop scheme only resists the interrelated nodes with DoS attack. Luk, *et al*. (2006), has described seven properties that are cardinally accepted for any broadcast authentication algorithm in wireless sensor network. By these seven properties which leads to resistant to compromised nodes, immediate authentication message set at irregular time interval periodwith high message entropy, less communication overhead, less power consumption in WSNs, increased wireless sensor network lifetime, low computation overhead and more robustness toward packet loss. Most current schemes satisfy almost all of them. The Digital signature will satisfy all the cardinal properties except low consumption overhead. In (Ning *et al*., 2008) Message specific puzzle has been proposed by Ning *et al*. which is used to mitigate the DoS attacks. Weak authenticator technique has been used on every broadcast message.

The weak authenticator is not a replacement of authentication approaches like Digital signature and Timed Efficient Stream Loss-tolerant Authentication; instead it is used to differentiate the forged broadcast messages. A sensor node receives a broadcast message and will check it with the weak authenticator first to ensure that it's valid. Then the sensor node will perform the signature verification or packet forwarding by either using Digital signature or TESLA. These approaches have two limitations: they require a computationally powerful sender in order to compute the puzzle solution and they cause a delay in sending packets to receiver. In Al-Momani *et al*. (2010) proposed a new scheme that allows the receiver sensor node to recognize forged message before message before verifying its authenticity in order to avoid performing many unnecessary operations. This prevents DoS from damaging the availability of the network and additionally reduces the delay that results from the verification itself.In Dong *et al*. (2008) has proposed to use Pre-authenticator filters to provide a first line of authentication before the main broadcast authentication such as Digital Signature and Timed Efficient Stream Loss-tolerant Authentication is applied.

This approach will follow group based or key chain based pre-authentication filter; which requires key distribution in re-grouping. The group based approach provides the possibility of compromised node within the group and results in communication overhead due to additional key management mechanism. Tan *et al*. (2009) demonstrated a solution that pursues to provide both confidentiality and authentication that resists the possible Denial of service attacks Dos, in order for code dissemination specifically which is the process of distribution new programs image over the wireless sensor network to update program versions. Hence this approach depends on the idea of chaining then relay in finding the cipher puzzle to avoid denial of service attack when compared to MSP in (Ning *et al*., 2008). They this is better than the Message Specific Puzzle due to chaining of hash results in previous packets. Huang *et al*. proposed a broadcast

authentication scheme in (Huang *et al*., 2008) called DREAM which stands for DoS Resistant Efficient Authentication Mechanism. This process which contains a false packet by frequently using authentication first and which nodes must verify the authenticity of the message before forwarding the packet and also its sends the small number packet to receiver node without verifying the packet; which reduces the overall delay. So the remote node gets the message more quickly. In this solution the sensors periodically exchange hello message with one hop neighbor, then the one hop neighbor size is included in each hello messages. Then these message must be signed and verified. This introduces an extra overhead. DREAM is used in MANET. In (Du *et al*., 2008; Ren *et al*., 2009 and Gan and Li, 2009) focused on environment in networks, the nodes know each neighbor node at least once in a while. In Ren *et al*. (2009) use the bloom filter to allows the node to a certain receiver is part of the network, but bloom filter which results in false positive, which provides additional security concerns. Similarly in research of (Du *et al*., 2008) depends on nodes to be verified with each other neighbor node in the network by using the sender specific one way chain. Keys in the chain are unique for each node then each receiver must verify the key according to which the message has been received from.

Martynov *et al*. has designed and implemented a preliminary Intrusion Detection System IDS for wireless sensor networks which protect the network from DoS described in (Martynov *et al*., 2007). In order to detect DoS attacks in networks, an anomaly detection system is used. The main goal of this system is to stop DoS attackers and communication through advisory nodes and continuing the communication through non-advisory nodes. So the system draws a baseline level of network traffic and determines whether the DoS attacks exist or not by comparing the traffic against the baseline.There is a broadcast authentication scheme for WSNs (wireless sensor networks) wherein a multiple user, DoS (Denial-of-Service) containment and signature-based broadcast authentication are utilized. A generic approach with a RRAS (Reputation-based Randomized Authentication Scheme) scheme is utilized to effectively manage the DoS (Denial-of-Service) attacks for the concerned broadcast authentication. The main advantage of RRAS (Reputation-based Randomized Authentication Scheme) scheme is that it is lightweight and is easily deployed on the sensor nodes.

Further, the scheme happens to be associated with a good reputation and effective risk management capabilities Qi Dong and Donggang Liu (2013). This proves to be a vital tradeoff between the containment of DoS (Denial-of-Service) attacks and the end-to-end delay aspect. Moreover, the scheme is flexible enough towards the DoS (Denial-of-Service) attacks and thereby the acceptance of end-to-end delay is justifiable. The storage cost can be further reduces to manage more broadcast users in the wireless sensor network (Gan and Li, 2009; Ning *et al*., 2008). Wang *et al*. (2007) proposed the dynamic window solution, it allow the nodes to cut off between first authentication mode and forward the first mode to get benefit of both. The Former mode, a node must verify the authenticity of the messages before forwarding it. Additive Increase Multiplicative Decrease AIMD is a feedback approach to control the network traffic. The most significant feature of AIMD is the congestion control, in which AIMD combines the linear increasing for the congestion control and exponential decreases the congestion occurs. The solution proposed in this paper is based on the window scheme proposed in (Wang *et al*., 2007). This model doesn't add any overhead to the network. Gan *et al*. (2009) proposed method based on the solution illustrated by (Ren *et al*., 2009) and uses the same idea of window but in addition they are used as randomized reputation. Similarly the solution requires additional communication overhead.

Notation Used in this paper

Notation	Attributes
M	Broadcast message
w	Window Size
Distance	Hop Counter
T_i	Time Interval

Nomenclatures

Terms	Abbreviation/Meaning
WSN	Wireless Sensor network
DoS	Denial of Service
DS	Digital Signature
TESLA	Timed Efficient Stream Low - tolerant Authentication
PKC	Public key Cryptography
DREAM	DoS Resistant Efficient Authentication Mechanism
IDS	Intrusion Detection System
AIMD	Additive Increase Multiplicative Decrease

Proposed System Overview

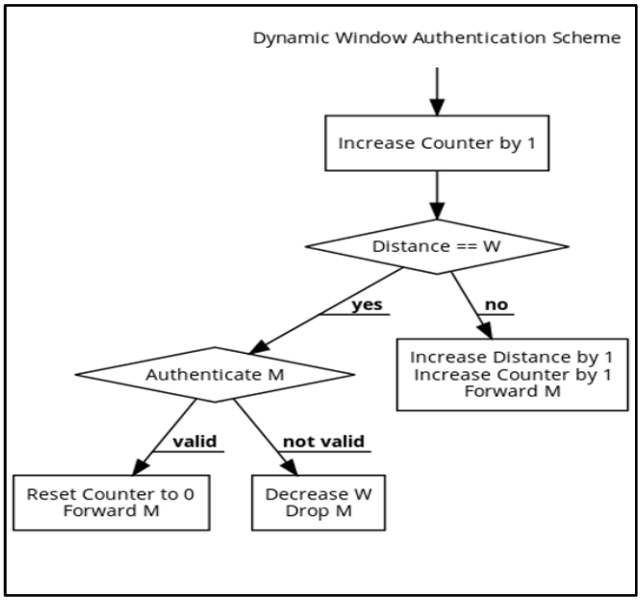

Figure 1. Proposed Solution

- The Base Station will send the broadcast message to the entire sensor nodes via multi-hop forwarding and some sensors will forward this message to others.
- The broadcast message could be a request or command. Broadcast authentication approach commonly used in the wireless sensor network with help of Digital Signature approach.

- The base station will sign the packets before sending it to destination and a sensor node need to perform Public Key Authentication to tell whether the message is sent from the base station originally or not. If it's a forged message, then the sensor node will immediately drop the message without performing any other operations.
- The attackers can launch Denial of Service (DoS) attacks on a wide range of the network. Attackers can inject a fake broadcast message to a pool of sensor nodes to verify some unnecessary computational process and delay the broadcast message.
- The broadcast message from sensor node is properly verified with help of broadcast authenticator.
- Attacks are assumed to be static: adversaries, as well as sensor nodes and base stations, stay in fixed locations throughout the attack. That is, the topology of the network is fixed. Attackers can choose their locations, or take multiple identities, but they cannot move during the attack.
- In addition, attackers can exploit the large network diameter to isolated farther node by fooling them to perform some unnecessary computational process using the time delay of broadcast messages.
- Other types of DoS attacks such as jamming or black hole attacks are not considered in this paper.

Proposed updated version of dynamic window authentication scheme

- Dynamic Window Authentication Schemeis mainly used to avoid the unnecessary verification of broadcast message and possibly it will reduce the Denial of service without introducing any additional overhead, forged message are dropped before verified.
- We need an indication for such forged messages are injected in broadcast message.
- The use of authentication-first mode or forward-first mode alone yields serious problems in network. Hence, each node is vulnerable to a specific attack.
- Authentication-first results in a longer broadcast delay in the network. Forward-first allows forged messages to pass, which spreads the fake message across the entire network.
- This will lead to Denial of Service available in entire network, by doing unnecessary computation of broadcast message in the network and increasing battery consumption, therefore decreasing the life time of the wireless sensor network.
- Our proposed solutions uses a dynamic window, this will make sure whether the sensor node need to forward broadcast messages before authenticating them (as this will build some trust among the surrounding networks in the environment), or it will authenticate the messages before forwarding them and will drop them if they're faked.
- In System Overview, we demonstrated clearly how the authentication process is carried out in Wireless Sensor Network as shown in Figure 1.
- The Dynamic Window Scheme is demonstrated in the following section in detail.

Authentication-First Scheme

When using this scheme, the message M is first authenticated after arriving to a new node. If the message is valid then it's forwarded to other neighbour nodes; if it's a fake, then the message is dropped immediately. This scheme alone will result in a considerable time delay, which is not affordable in time-sensitive applications.

Forward-First Scheme

In this scenario, a message M is first forwarded to the neighbour nodes before validation. After that, the authenticity of the message is checked and the message is then processed if it is valid. Using this method on its own will cause faked messages to be spread across the entire sensor networks, consuming the network's energy. Although the nodes will eventually drop faked messages after the fail of verification, the damage has already been made to the network**.**

The Dynamic Window

The Dynamic Window will provide a protection layer against Denial of Service attacks and will ensure that they do not persist in the network. The Dynamic Window approach will check the authenticity of the message M before it is forwarded only in a certain case. In our algorithm each sensor node keeps a parameter w called window size and stored locally. Distance is a message-specific parameter that holds the total number of hops M has travelled through in the network without being authenticated in them so far. Counter is also a message-specific parameter that holds the number of hops the message M has travelled since the last authentication-first on M. M is only verified when its Distance parameter is equal to the window size of the current node. This is done to ensure the minimization of time delay and energy consumption.If Distance = window Size, then the node should proceed with authentication process and verify the message.After that, we need to reset M's Counter to zero to indicate that the message has been authenticated just now. If the message is a fake, we just drop it and decrement the node's window size by 1.When we identify a faked message we update the window size according to the following:

$w_{new} = w_{old} - 1$

If Distance ≠ window Size, we just forward the message after increasing its Counter and Distance by 1.

Pseudo Code for Proposed Algorithm

```
Dynamic Window Algorithm
Parameters: node N, message M
if(M.Distance == N.windowSize)//authentication-first
authenticate M
if M is fake
drop M
increase fake counter by 1
if(N.windowSize> 1) //N.windowSize can be decreased
decreaseN.windowSize by 1
else//M is valid
forward M to the next node(s)
resetM.Counter to 0
else//forward-first
forward M to the next node(s)
increaseM.Distance by 1
increaseM.Counter by 1
```

Figure 2. Proposed Algorithm Structure

- This algorithm will take constant time, as all of its operations take constant time.
- The window Size of all nodes is initialized to the maximum number of possible hops.
- This approach will save much of the time and energy required to verify messages at every node, thus it will minimize time delay and lengthen the life of the whole network.
- Appropriately, in this way only a small portion of the network will be affected by the Denial of Service (DoS) attacks.

Security Analysis and Evaluation

As it was clearly indicated before, the dynamic approach prevents attackers from launching DoS attacks on the network; it will also help in avoiding rapid changes in the network due to extreme scenario.The window size w is stored locally in each node as demonstrated in the early part of the algorithm.
Denial of Service attacks can affect the network in many ways such as:

- Draining the energy of sensor nodes.
- Causing significant delay in the network due to the unnecessary verification procedures.
- Most importantly it will reduce the life-time of the Wireless Sensor Networks.
- This will automatically result in the network efficiency being reduced.

The proposed dynamic window can reduce the Denial of Service attacks in the network to involve only a small portion of sensors that have a chance to be affected by the attackers. The new proposed algorithm can reduce the effect of DoS attacks in the network by saving sensors energy and minimizing the average delay of the authenticated broadcast message. This will restrict the spreading of forged message in the network. In this section we have studied the proposed algorithm by comparing its performance to authentication-first scheme and forward-first scheme. Simulation results show some other factors which might affect the proposed algorithm. Some of the factors are

- Density of sensor in Wireless sensor network.
- The intensity of Dos attacks.

The two main characters which are used to evaluate the newly proposed algorithm:

Degree of energy saving in the wireless sensor networks

Evaluates in terms of the portion of nodes that have received forged message and the amount energy consumed to verify if the message is forged for each of them.Also the portion of nodes which forwards the forged message. This portion will determines how the dynamic window scheme is more effective in terms of reducing the Dos attacks in a wireless sensor network.

Average broadcast delay in authenticated message

Evaluates in terms of the number of verifications performed on each message before sending it to the base station and time required for each verification process.

Environmental Setup

In our experimental simulation, we have generated a network with a huge number of sensor nodes; in which the sensors are deployed randomly, this forms a sparse network. This network structure is more appropriate to the environment and the problem we are trying to solve; which is the minimization of delay and energy consumption in the network. The mentioned structure also helps in making the performance of the algorithm more visible. In dense network each sensor node is closely connected with the neighbor node. A large number of sensors are connected via single hops and messages are exchanged using the shortest paths in the network.

- Mixed authentication message attacking model (Wang *et al*., 2007) is one of the well-known realistic model in most of the real-time applications.
- The window Size of all nodes was initialized to the maximum number of possible hops.
- The window size is only updated if it can be decreased, meaning that it is larger than 1.
- The simulation is done according to the flowchart inFigure 3.
- The flowchart is concerned with a single message at the time.
- In the beginning, the delay is set to 0.
- The delay in the authentication-first scenario is 2 times the number of verifications.
- The output of fake/authentic ratios, time delay and energy consumption is done separately.
- The *hack*parameter indicates whether the message is originally a fake or a valid message.
- The *pre-crnt, delay* and *CURRENT_TIME* variables are used to extract the net delay of the network nodes.
- *WindowSize*, *dist* (Distance) and *counter* (Counter) are used as mentioned earlier in the previous sections.
- *fake* and*auth*parameters are counter for faked and authentic occurrences respectively.

RESULTS AND DISCUSSION

In early mentioned attacking models such as mixed authentic message model in which to identify the intensity of Dos attacks:

$$\text{Dos Attack Intensity} = \frac{\text{Number of Faked Messages}}{\text{Number of Authentic Messages}}$$

Our algorithm clearly shows the energy consumption and average broadcast delay of authenticated messages varying the DoS attacks in the network. From this we can easily evaluate the intensity of DoS attacks. Energy consumption of forged messages in with respect to DoS attacks intensities can be found by calculating the portion of nodes that received forged message and the portion of nodes that forwarded the forged messages. The energy consumed by broadcast authentication approaches such as Digital Signature and Timed Efficient Stream low–tolerant Authentication TESLA and many unnecessary sending/receiving operations are considered as an overhead waste of Network Resources.

The portion of forged messages received by the sensor nodes shows how much of the forged messages spread throughout the network, the amount of energy consumed during receiving and verifying the forged messages in the communication overhead. Those portions can be calculated by the below equation:

$$\text{Portion of Received Forged Messages} = \frac{\sum \text{number of Received Forged Messages}}{\text{Performed Receiving Actions}}$$

The portion of forwarded forged messages consumes a considerable amount of energy in communication and shows the network's ability to resist the spreading of forged message within itself. This can be calculated according to the following equation:

$$\text{Portion of Forwarded Forged Messages} = \frac{\sum \text{number of Forwarded Forged Messages}}{\text{Performed Forwarding Actions}}$$

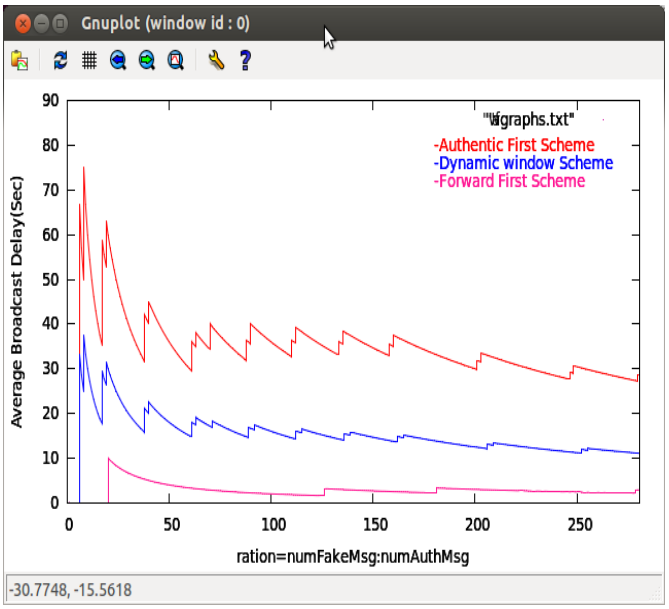

Figure 3(a). Average Delay under attacks with respect to the ratio of fake messages to authentic messages

Average broadcast delay for the authentic messages under various Denial of Service intensities. The window scheme proposed in (Wang *et al*., 2007) introduces less amount of delay when compared to using of authentication first mode purely and it alternates authentication-first and forward-first modes. In our experiments, we compared the average broadcast delay our algorithm produced for authentic messages and broadcast delay produced in authentication-first and forward-first schemes.Figure 3(a) shows how our proposed algorithm with Authentication approach reduces the delay of broadcast messages by varying the Denial of Service attacks intensities as shown in the graph clearly.We can compute the average broadcast delay by counting the number of authentications on each message in the sensor nodes after transmitting the message from base station. We can assume that 2 seconds are needed for a single verification process in the network.The delay is calculated by the following formula:

$$\text{Delay} = 2 * \text{Number of verificationprocesses}$$

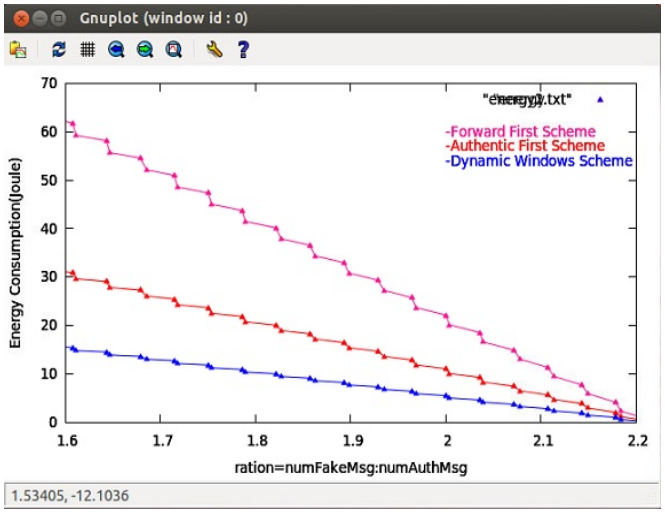

Figure 3(b). Energy saving: Portion of nodes receiving/forwarding faked messages under attacks of various intensities

Figure 3(b) shows Energy consumption of faked messages under various DoS attacks intensities. We evaluate the energy saving in simulation by calculating the portion of nodes that received faked messages, and portion of nodes that forwarded faked messages, for different DoS attacking intensities. Beside the energy consumed by the broadcast authentication approach – such as digital signature – many unnecessary sending/receiving operations are considered to be additional overhead that wastes the network resources. The portion of nodes receiving faked messages shows how much of the faked messages are spread over the network which indicates the amount of receiving and verification power loss, communication overhead, and other network resources loss due to forged messages.

Conclusion

Broadcast authentication in wireless Sensor Network achieved by using Digital Signature and Timed Efficient Streamed Low-tolerant Authentication TESLA is still vulnerable because the Denial of Service attack is persisting in network. This will make the sensor nodes battery consumption increase by enforcing the sensor nodes to perform unnecessary verification. Since broadcast authentication is more difficult in wireless sensor networks, the above can't be completed in a real-time environment. Hence, this will not provide the guarantee needed for the installed application will execute correctly without any possible attacks.In this paper we proposed an updated version of Wang algorithm that prevents the Denial of Service in Wireless Sensor Network by using a Dynamic Window Scheme. It combines authentication-first and forward-first, in which our algorithm decides if the message will be authenticated first or forwarded first that depend on the security provided in the environment. The performance evaluation of proposed algorithm can reduces the significance of DoS attacks. The proposed algorithm will ensure to contain the attack in small portion of the network, therefore saving the energy consumption of sensor nodes and minimizing the delay in broadcast messages.

REFERENCES

Al-MomaniIman, Karejah Ola and Abdullah Lamya, 2010, Reducing the Vulnerability of Broadcast Authentication against DoS Attacks in Wireless Sensor Networks, Mediterranean Journal of Computers and Networks.

Dong, Q., D.Liu and P. Ning, 2008. "Pre-Authenticator Filters: Providing DoS Resistance for Signature-Based Authentication in Sensor Networks", WiSec'8: ACM, pp. 2-12.

Du,X., M. Guizani, Y. Xiao and H. Chen, 2008."Defending DoSAttacks on Broadcast Authentication in Wireless Networks", IEEE Communications Society.

Gan,X. and Q. Li, 2009."A Multi-user DoS-containment Broadcast Scheme for Wireless Sensor Networks", in 2009 International Conference on Information Technology and Computer Science, IEEE Computer Society.

Gura, N., A. Patel, A.Wander, H. Eberle and S. Shantz, 2004."Comparing Elliptic Curve Cryptography and RSA on 8-bit CPU", In CHES 2004, Cambridge, MA.

Huang, Y., W. He, K. Nahrstedt and W. C. Lee, 2008. "DoS-Resistant Broadcast Authentication Protocol with Low End-to-End Delay", Computer Communication Workshops.

KesselmanA.and Y.Mansour, 2003. "Adaptive AIMD Congestion Control," Annual ACM Symposium on Principles of Distributed Computing.

Luk, M., A. Perrig and B. Whillock, 2006. "Seven Cardinal Properties Broadcast Authentication", SASN'06: ACM.

Martynov, D., J. Roman, S.Vaidya and H. Fu, 2007."Design and Implementation of an Intrusion Detection System for Wireless Sensor Networks", IEEE EIT Proceedings.

Ning, P., A.Liu and W. Du, 2008. "Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks", ACM Transaction on Sensor Networks, Vol. 4, No. 1.

Perrig, A., R. Canetti, J. D. Tygar and D. Song, 2000."The TESLA Broadcast Authentication Protocol", work was done at UC Berkeley and IBM Research.

Qi Dong and Donggang Liu, 2013."Providing DoS Resistance for Signature-Based Broadcast Authentication in Sensor Networks.

Raymond, D. R. and S. F. Midkiff, 2008. "Denial-of-service in Wireless Sensor Networks: Attacks and Defenses", IEEE CS, Vol. 08.

Ren, K., S. Yu, W. Lou and Y. Zhang, 2009. "Multi-User Broadcast Authentication in Wireless Sensor Networks", *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 8.

Rivest, R. L., A. Shamir and L. Adleman, 1978."A Method For Obtaining Digital Signatures and Public-KeyCryptosystems", Communications of the ACM, 21(2): 120-126.

Stallings, W. 2014.Network Security Essentials, Pearson Prentice Hall 5th edition.

Tan, H., D. Ostry, J. Zic and S. Jha,2009. "A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Networks", WiSec'09: ACM.

Wang, R., W. Du and P. Ning,2007. "Containing Denail-of-Service Attacks in Broadcast Authentication in Sensor Networks," MobiHoc'07: Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing.

Wood, A. D. and J. A. Stankovic, 2002."Denial of Service in Sensor Networks," IEEE.

****