ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

Secure Authentication Scheme against DoS Attacks

M.Nagateja[1], D.Venkata Subbaiah[2]

PG Student, Department of CSE, Andhra University, Visakhapatnam, India

Research Scholar, Department of CSE, Andhra University, Visakhapatnam, India

ABSTRACT: Public-key cryptography operations are heavy to resource constraint nodes. So the attackers can cause a problem to a sensor node but forcing it to perform a large number of false cryptographic operations. Therefore, attackers can cripple a sensor node by forcing it to perform a large number of false PKC operations. In this paper, We propose a fully distributed and effective scheme that randomly drops and extra key cryptographic request messages beyond its processing capability. Our scheme is not only resistant to PKC-based DoS attacks, but also energy-efficient **.**Timed Efficient Stream Loss-tolerant Authentication (TESLA) and digital signature are security implementations of broadcast authentication in Wireless Sensor Networks (WSNs). This paper provides a hybrid solution between prevention and detention scheme, called as Combined prevention and Detection scheme. The prevention part is based on the dynamic window scheme installed at each sensor node. The detection part adopts the Fuzzy Logic Intrusion Detection Scheme (FL-IDS) installed at monitor nodes. Both parts work coherently where the detection part relies on predefined information provided by the prevention part.. This scheme is not only resistant to PKC-based denial-of-service attacks, but also energy-efficient. To prevent and detect DoS attack and 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.

I. INTRODUCTION

A Wireless Sensor Network is defined as a large set of tiny sensor nodes, they can vary from few to several hundreds or thousands. They have the capabilities of sensing, computational and communication .Like many advanced technologies, the origin of WSNs is found in military and heavy industrial applications. The Sound Surveillance System , developed by the United States Military in the 1950s, during the Cold War, to detect and track Soviet submarines, is the ancestor of modern WSNs.

Later, in the early 1980s, the United States Defense Advanced Research Projects Agency (DARPA) launched the Distributed Sensor Networks (DSN) program to examine the potential benefits in implementing distributed wireless sensor networks, which was followed by the Sensor Information Technology program that provided the present sensor networks with new capabilities, such as ad-hoc networking, dynamic querying and tasking, reprogramming and multi-tasking. Now a days, universities and governments are aware and using WSN s in many applications such as monitoring air quality, detection of forest fire, weather stations, factory automation. At the time, all the above military, science/technology and industrial applications were based on bulky, expensive sensors with limited performance, functionality and scalability. Major advances in micro electromechanical systems , CMOS based semiconductor devices, networking protocols and energy storage technologies, dramatically reduced the high deployment and mainly maintenance cost and leveraged the widespread adoption of WSNs into a broader range of applications, including home automation, smart environments, continuous medical monitoring systems, environmental control and many others. In short, we can presume that future WSNs will form the building blocks of the Internet of Things , changing our everyday life in unprecedented and unanticipated ways.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

II. METHODOLOGY

Many approaches were proposed to reduce unnecessary verification to secure broadcast authentication and forwarding of broadcast message. Some of them targeted for containing the impact of DoS attacks to include a small portion of the network. Whereas there are some that attempted to keep such attacks from propelling against the broadcast authentication approaches. As of now, there is no such scheme that can identify and avoid DoS attacks from abusing the broadcast authentication process. Hence, a combined scheme that can counter-act and distinguish DoS attacks, especially those attacks that start against the broadcast authentication within the WSN. The prospect scheme in this analysis is named Combined Prevention Detection based Scheme (CPDS). It is focused on the two main sections:

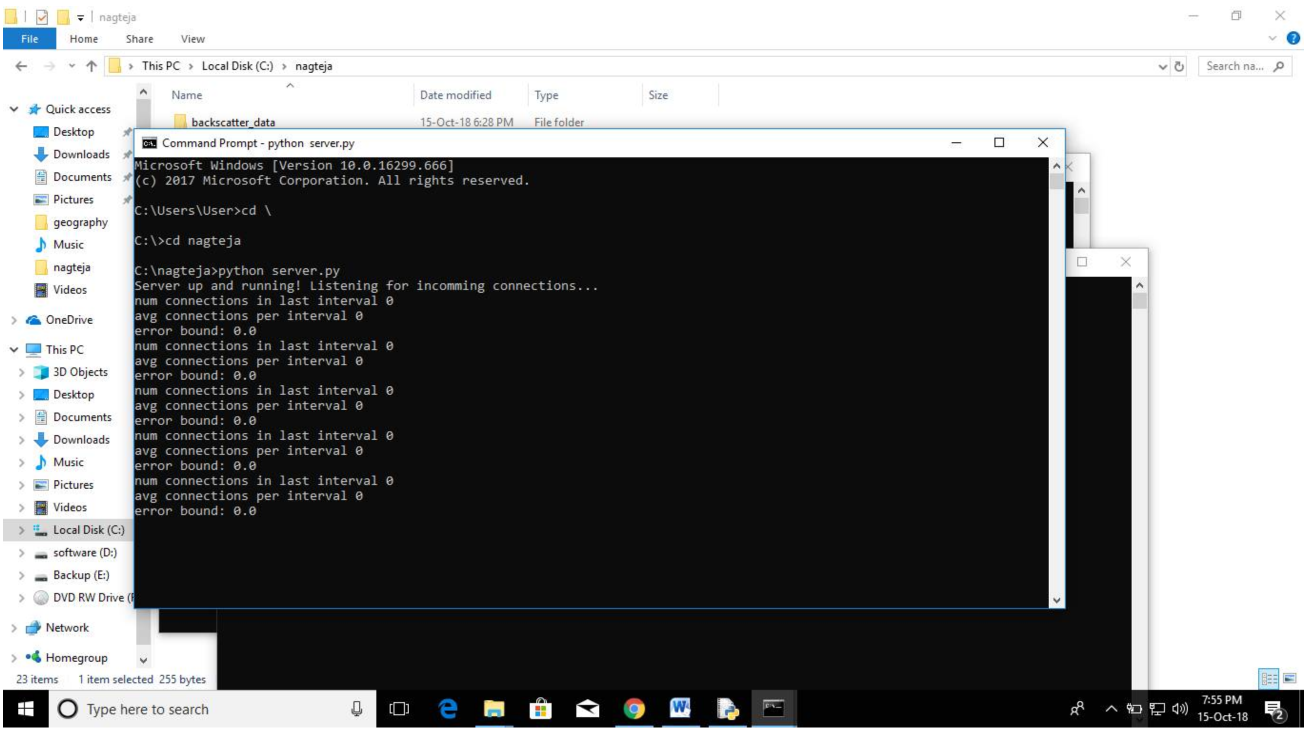
1. Prevention part

2. Detection part

In the prevention part, the dynamic window scheme proposed is used as first line of defense that can decrease the harm caused due to DoS attacks to include just a small portion of the network. This scheme is installed in every sensor node. In the detection part, for each monitor node a proposed Fuzzy Logic based Intrusion Detection Scheme (FL-IDS) is used as second line of defense. This second resistance approach relies on the accessible data created by the dynamic window system and uses the Fuzzy Logic Inference System (FIS) so as to settle on a right decision about the attacker.

III. RESULTS

Fig 1: Python server.py is executed in Command prompt and the result is shown above and now the server is listening for the incoming connections.We can see the number of connections in last interval, average connections per interval, error bound.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

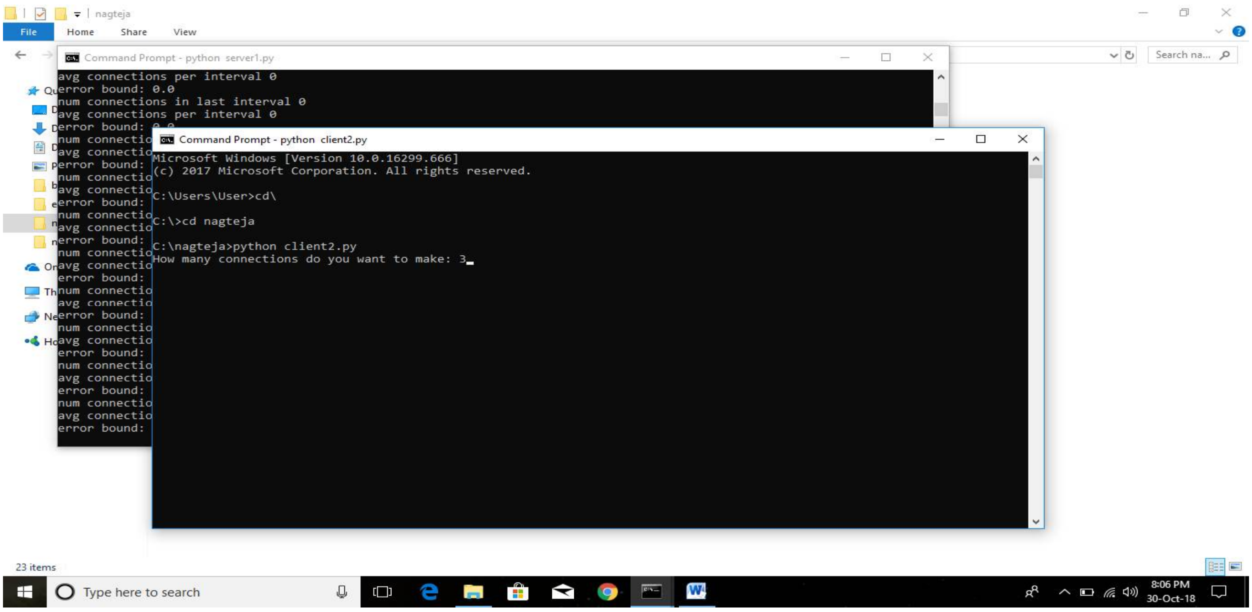
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

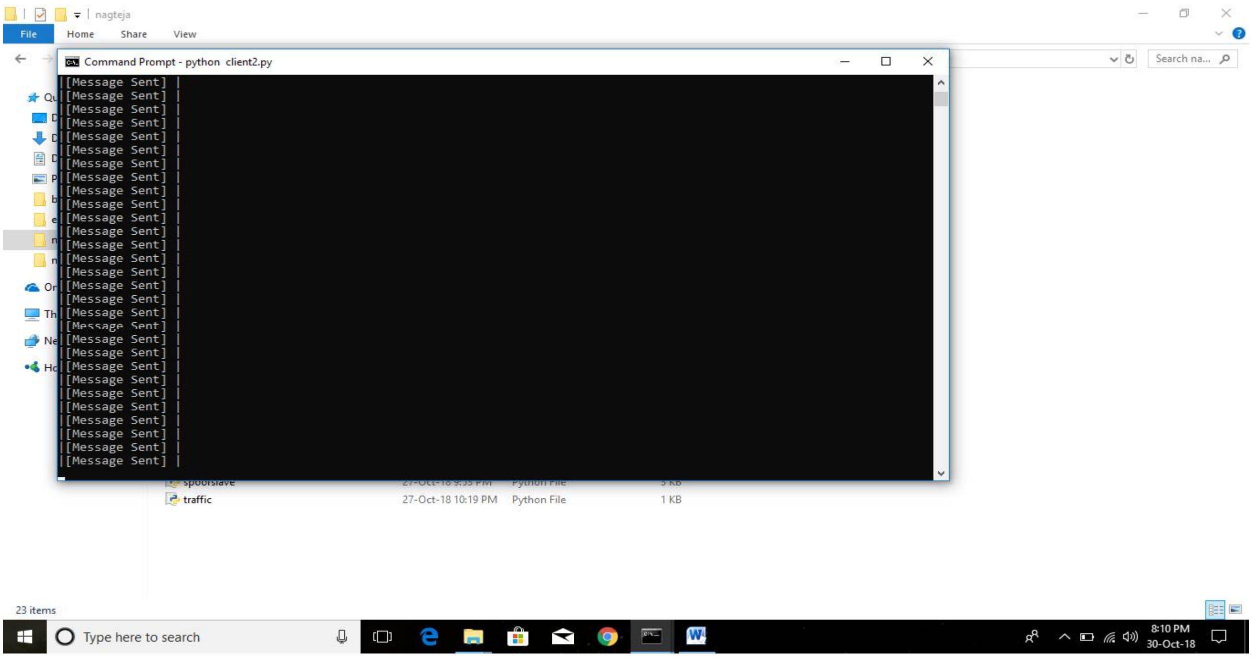
Vol. 6, Issue 10, October 2018

Fig 2 client2.py is executed in the command prompt and the result is shown as “How many connections do you want to make?”



In the below screen continuous flow mesages .

Fig 3 The continuous messages are being displayed which are above the limit in Client2.py



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

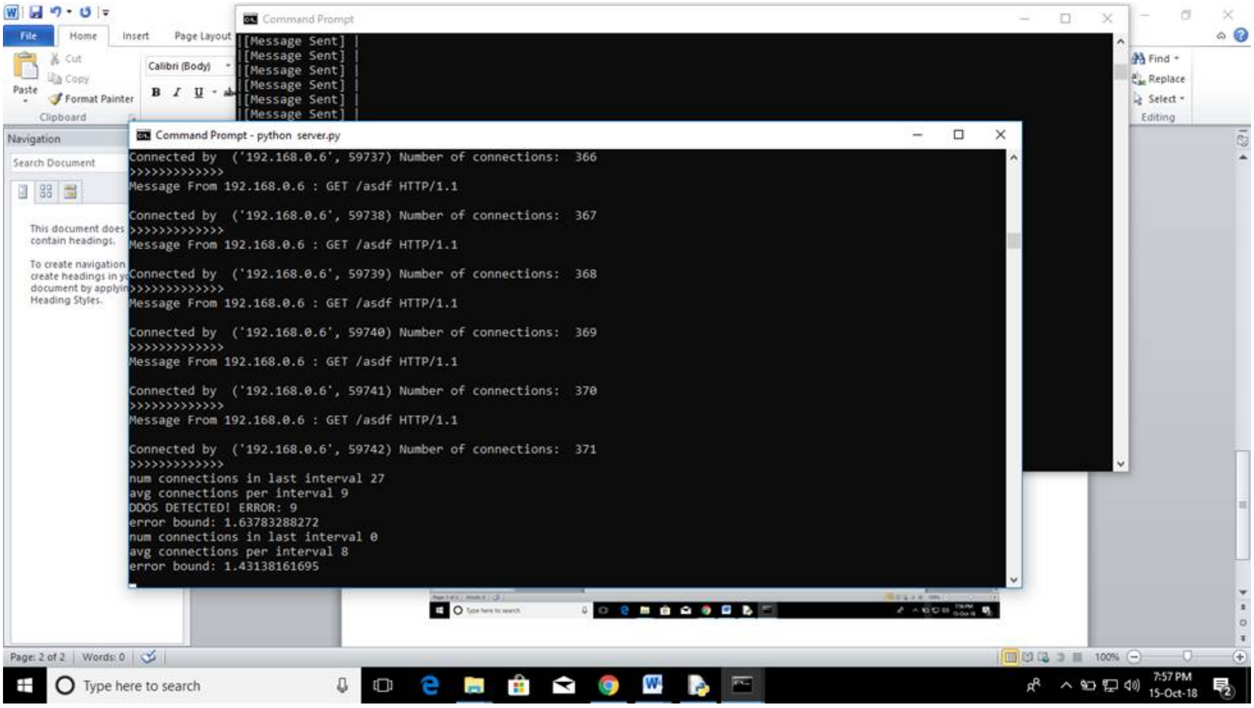
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

Fig 4:Detection of the dos attacks are shown in the screen in server side when the client2 system is stopped and the information i.e, number of connections in last interval, average connections per interval, DDOS detected errors error bound is been found in command prompt.



IV. CONCLUSION

Authentication remains a very challenging area in wireless sensor networking. There is no turn-key solution available in order to thoroughly secure WSN networks with minimal power and communications costs.

In this Project, an authentication scheme based on sinusoidal functions which operate as pseudo random number generators was introduced. This scheme prevents the disclosure of the sensor nodes' identities and enhances the network's privacy, since each node has not a specific id that easily can be intercepted, but uses a sin function instead. All legitimate nodes of the network share their authentication functions by design and can be mutually authenticated at any time, avoiding this way a variety of attacks. The extension of the present implementation is required for the future work For future work, in order to support dynamic addition of new mobile sensor nodes and testing the framework under a more dynamic network. Also experiments should be contacted based on specific attack scenarios. Finally further implementation and trail work is essential to assess the proposed scheme, in terms of communication and energy efficiency.

REFERENCES

1. L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey,"Computer Networks.
2. "Centre for Communication Systems Research," University of Surrey.
3. I. Akyildiz, W. Su and E. Cayirci, "Wireless sensor networks: a survey,"Computer Networks
4. J. Tillison, "An introduction to wireless sensor network concepts," Electronic.

5.W. Dargie and C. Poellabauer, Fundamentals of Wireless Sensor Networks:Theory and Practice, West Sussex, United Kingdom: John Wiley & Sons Ltd.,
6.E. C. Whitman, "Sosus, the Secret Weapon of undersea surveillance," Undersea Warfare - The official website of the U.S. Submarine Force.
7.S. Kumar and D. Sepherd, "SensIT: Sensor Information Technology for the Warfighter," Proc.
8. N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks,"in Proceedings .
9."Android Developers," Google Inc., [Online]. Available: http://developer.android.com/images/system-architecture.jpg.
10."Android Developers," Google Inc., [Online]. Available: http://developer.android.com/sdk/index.html.
11. Oracle America Inc., [Online]. Available: http://www.oracle.com/technetwork/java/javase/downloads/index.html.
12. "JmDNS | Free Communications software," Apache, [Online]. Available: http://sourceforge.net/projects/jmdns/.