IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Securing Data In Network Traffic Using Pattern Matching

Mr. k. Tarun (M.C.A). Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal

Mr. K.R. Harinath M. Tech, (Ph.D.) Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal.

Abstract

A wireless sensor networks consists of light weight, low power and small size of sensor nodes. The areas of applications of sensor networks are military, healthcare, forest fire detection, etc. In WSN, sensor nodes process the measured data and transmit it to base station through a wireless channel. The Base Station collects data from all the nodes, and analyzes this data to draw conclusion about the activity in the area of interest.

Sensor device can be divided into two classes as event driven and continuous dissemination. Our project belongs to event driven, where routing protocols are usually implemented to increase energy savings

1. INTRODUCTION

1.1 Introduction

Large-scale adoption of Network Function Virtualisation (NFV) facilitates easy realisation, deployment, and management of advanced network functions (aka middleboxes) for enterprises. Under this paradigm, cloud data centres become major NFV vendors [1]. Traditionally dedicated and tightly coupled hardware/software is transformed into composable software middlebox modules, which can run on commodity cloud instances with unlimited scalability. Such a technology shift also raises crucial privacy concerns, because the traffic of enterprises is re-directed and exposed to cloud data centres [2], [3]. Although HTTPS is widely adopted, commercial middlebox services intercept and decrypt the traffic to retain advanced network functions like deep packet inspection (DPI) [4]. To address this privacy concern, privacy-preserving middleboxes [5]–[14] have received much attention; these middleboxes are designed to process encrypted traffic against encrypted rules without decryption. As a result, sensitive traffic payloads and proprietary middlebox rules are protected without sacrificing the underlying operations of network functions, such as pattern matching, header inspection, and regular expression. Existing studies in this field can be classified into two categories, i.e., software-based solutions [5]–[10] and hardware-based solutions [11]–[14]. Unfortunately, neither of them are practically deployable due to efficiency and/or security issues. Limitations of prior work. Mainstream software-based solutions [5]–[10] adapt a cryptographic technique named searchable encryption [15], which allows middleboxes to match encrypted patterns extracted from

rules against encrypted string streams (i.e., tokens) parsed from traffic payloads. Those designs are communication inefficient, because traffic payloads need to be tokenised into string streams via sliding windows in varied sizes (i.e., enumerating the sizes of all specified patterns). As shown in prior work [5], [6], [9], [10], [16], such cost can be tens of times to the original packet size. Consequently, long latency is inevitably introduced in token transmission, which is not acceptable in most networked applications. Besides, high I/O consumption between the enterprise and cloud greatly increases the capital cost of data transfer. Hardware-based solutions [11]–[14] rely on hardware enclave (i.e., Intel SGX) to execute middlebox functions in a trusted environment, in which traffic is fed into the enclave and processed within it. Using SGX brings benefits on efficiency and functionality for secure middleboxes, but sidechannel attacks against SGX [17]–[19] make such adoption questionable. Contributions and technical overview. To tackle the above limitations, in this paper, we aim to propose practical cryptographic protocols for a wide range of pattern matchingbased secure middleboxes. Our design expects to offer convincing performance in both time and communication towards network environments, while ensuring cryptographic protection for rules and traffic payloads. As mentioned, existing designs based on searchable encryption fall short of achieving bandwidth efficiency. To overcome this bottleneck, we observe that a cryptographic

2. Literature Survey

• **[1] J. Shad and S. Sharma, "A Novel Machine Learning Approach to Detect Phishing Websites Jaypee Institute of Information Technology''**Many phony websites have emerged on the World Wide Web in recent years with the intention of hurting people by obtaining their private data, including account IDs, user names, passwords, etc. Phishing is a type of social engineering attack that primarily targets mobile devices today. That can lead to losses on the financial front. In this article, we discussed a variety of detection methods that make use of URL and hyperlink properties to distinguish between websites that are broken and those that are not. There are six basic methods: the heuristic, the blacklist, the fuzzy rule, machine learning, image processing, and the CANTINA-based method. It provides a thorough analysis of the phishing problem, a current machine learning solution, and future research on the hazards posed by phishing utilizing a machine learning**approach.**

[2] Y. Sönmez, T. Tuncer, H. Gökal, and E. Avci, "Phishing web sites features classification based on extreme learning machine," 6th Int. Symp. Digit. Forensic Secur. ISDFS - Proceeding: Phishing is a widespread tactic used to trick gullible people into disclosing their personal information by using phony websites. Phishing website URLs are designed to steal personal data, including user names, passwords, and online financial activities. Phishers employ websites that resemble those genuine websites both aesthetically and linguistically. Utilizing anti-phishing methods to identify phishing is necessary to stop the rapid advancement of phishing techniques as a result of advancing technology. A strong tool for thwarting phishing assaults is machine learning. The characteristics and machine learning-based detection methods are surveyed in this work.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

Existing System, many energy consumption algorithms have been proposed to optimize and improve original RPL routing algorithms (LEACH, SEP, DEEC). System in WSN routing algorithms for energy heterogeneous scenarios, Stable Election Protocol(SEP) considers two level energy heterogeneity in Low Energy Adaptive Clustering Hierarchy (LEACH) like Cluster Head(CH) role rotation environment's proposes weighted election probabilities based on initial energies of the nodes to give energy rich nodes more chances of becoming CHs.

The Dual MOP-RPL, which allows nodes with different MOPs to communicate gracefully in a single netw1ork while preserving the high bi-directional data delivery performance, was established to solve this

problem. None of these studies have investigated RPL load balancing problems over a real multi-hop LLN test bed, however. In the existing system, many energy consumption algorithms have been proposed to optimize and improve original RPL routing protocol. Gaddour, for example, proposed the CO-RPL, which functions by using multiple route selection to improve the original RPL object function. CO-RPL exhibits better energy consumptions and packet pass rates than original RPL, but packet congestion and control packet flooding are still possible in large-scale wireless sensor networks. Zhang established a new RPL routing object function based on energy-efficiency, but only energy conservation (not energy balancing) is considered during routing.

3.1.1 Disadvantages of Existing System

Energy Efficiency is very less

No proper Cluster head selection

3.2 Proposed System

A Novel routing algorithm named symmetric hidden vector encryption (SHVEis presented, which considers nodes traffic requirements along with its energy levels by making CH selection.

The CH Selection in SHVE is based on the CH role rotation approach, where the node *i* becomes CH in the current round *r*, It the random number selected by the Node *i* is less than the threshold T(*i*,r).

$$\boldsymbol{T(i,r)} = \begin{cases} \dfrac{\boldsymbol{P_i(r)}}{\boldsymbol{1 - P_i(r)\left(r \bmod \frac{1}{P_i(r)}\right)}} & \boldsymbol{if\ node\ i} \\ \boldsymbol{\in G(r)} \end{cases}$$

WhereP_i (r) is the CH selection probability for node *i* during round r. G(r) is a set of eligible nodes for the round r, where the rotation for node I to become eligible again is $\frac{1}{P_i(r)}$.

3.3 Methodology

1.Source Module

In this module, the service provider will browse the data file and then send to the particular receivers. Service provider will send their data file to Base Station and Base Station will connect to clusters, in a cluster highest energy sensor node will be activated and send to particular receiver (A, B, C…)..

2. Base Station

The Base station manages a multiple clusters (cluster1, cluster2, cluster3, and cluster4) to provide data storage service. In cluster n-number of nodes (n1, n2, n3, n4…) are present, and in a cluster the sensor node which have more energy considered as a cluster head and it will communicate first. In a router service provider can view the node details, view routing path, view time delay. Base Station will accept the file from the service provider, the cluster head will select first and it size will reduced according to the file size, then next time when we send the file, the other node will be cluster head. Similarly, the cluster head will select different node based on highest energy. The time delay will be calculated based on the routing delay.

Cluster

In cluster n-number nodes are present and the clusters are communicates with every clusters (cluster1, cluster2, cluster3 and cluster4).In a cluster the sensor node which have more energy considered as a cluster head. The service provider will assign the energy for each & every node. The service provider will upload the data file to the router; in a router clusters are activated and the cluster-based networks, to select the highest energy sensor nodes, and send to particular receivers.

3. Receiver (End User)

In this module, the receiver can receive the data file from the service provider via Base station. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

4 Architecture

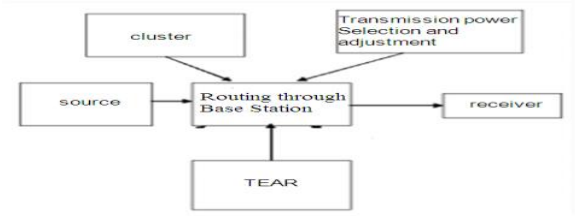
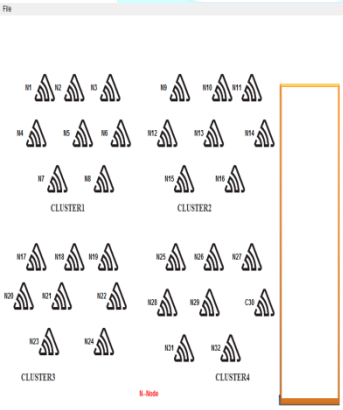


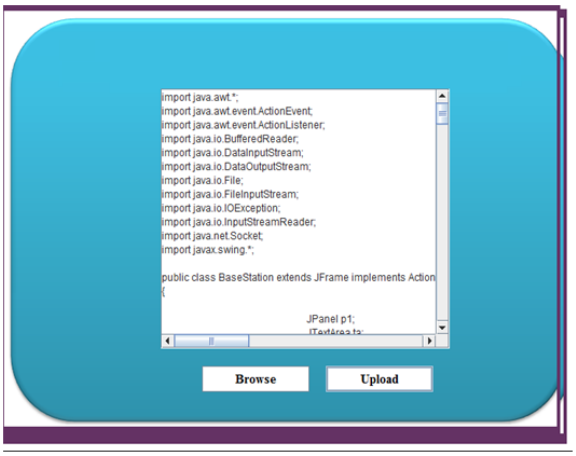
Fig 1: Frame work of proposed method

5 RESULTSSCREEN SHOTS

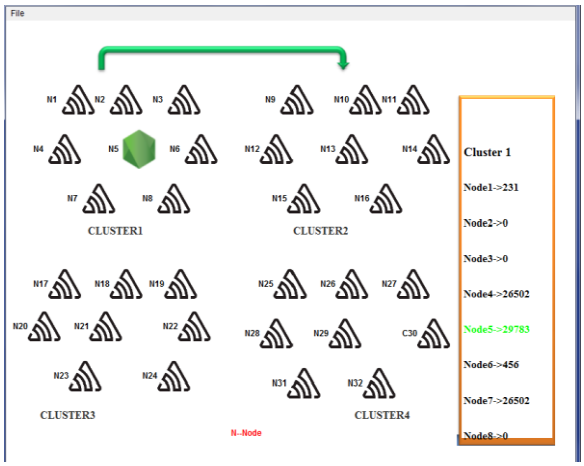
Home Page:



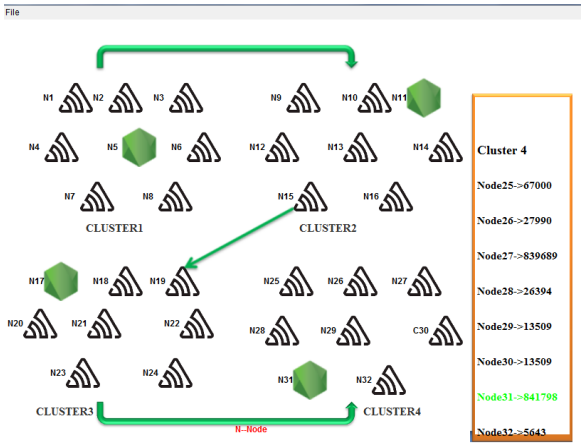
Upload Data:



Cluster:



Result:



6. CONCLUSION

In this paper, we design a protocol that allows outsourced middleboxes to perform pattern matching over encrypted traffic. We first design a customised SHVE scheme (SHVE+) and then build an encrypted pattern matching protocol based on it to protect network traffic and middlebox rules during the pattern matching process. Next, we design a secure filtering protocol to accelerate the pattern matching process. We implement our protocol, and our evaluation on real-world rulesets and traffic dump illustrates its advantages in terms of bandwidth, inspection delay, throughput and deployment cost compared to the latest arts.

7. References

[1] S. Tanwar, N. Kumar, and J. J. Rodrigues, "A systematic review on heterogeneous routing protocols for wireless sensor network," Journal of network and computer applications, vol. 53, pp. 39-56, 2015.

[2] G. Smaragdakis, I. Matta, and A. Bestavros, "SEP: A stable election protocol for clustered heterogeneous wireless sensor networks," in Second international workshop on sensor and actor network protocols and applications (SANPA 2004), 2004.

[3] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," Wireless Communications, IEEE Transactions on, vol. 1, pp. 660-670, 2002.

[4] L. Qing, Q. Zhu, and M. Wang, "Design of a distributed energyefficient clustering algorithm for heterogeneous wireless sensor networks," Computer communications, vol. 29, pp. 2230-2237, 2006.

[5] H. Zhou, Y. Wu, Y. Hu, and G. Xie, "A novel stable selection and reliable transmission protocol for clustered heterogeneous wireless sensor networks," Computer communications, vol. 33, pp. 1843- 1849, 2010.

[6] D. Sharma, A. P. Bhondekar, A. Ojha, A. Shukla, and C. Ghanshyam, "A traffic aware cluster head selection mechanism for hierarchical wireless sensor networks routing," in IEEE Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on, 2016, pp. 673-678.

[7] M.-Y. Wang, J. Ding, W.-P. Chen, and W.-Q. Guan, "SEARCH: A stochastic election approach for heterogeneous wireless sensor networks," Communications Letters, IEEE, vol. 19, pp. 443-446, 2015.

[8] S. Choy, B. Wong, G. Simon, and C. Rosenberg, "The brewing storm in cloud gaming: A measurement study on cloud to enduser latency," in Proc. ACM 11th Annu. Workshop Netw. Syst. Support Games, 2012, pp. 1–6.

[9] D. Delaney, T. Ward, and S. McLoone, "On consistency and network latency in distributed interactive applications: A surveyparti," Presence: Teleoperators Virtual Envir., vol. 15, no. 2, pp. 218–234, 2006.

.

.