Monitoring Connectivity of Internet of Things Device on Zigbee Protocol

By Deris Stiawan

Monitoring Connectivity of Internet of Things Device on Zigbee Protocol

Conference Paper · October 2018
DOI: 10.1109/ICECOS.2018.8605225

6 authors, including:

Benni Purnama
STIKOM Dinamika Bangsa Jambi

Kurniabudi Kurniabudi
STIKOM Dinamika Bangsa, Jambi

Rahmat Budiarto
Surya University

Deris Stiawan
Universitas Sriwijaya

Monitoring Connectivity of Internet of Things Device on Zigbee Protocol

Benni Purnama
Department of Computer Engineering
STIKOM DinamikaBangsa Jambi, Indonesia
bennipurnama@stikom-db.ac.id

Sharipuddin
Department of Computer Engineering
STIKOM Dinamika Bangsa Jambi, Indonesia
sharip-udin@yahoo.co.id

Kurniabudi
Department of Computer Engineering
STIKOM Dinamika Bangsa Jambi, Indonesia
kbudiz@stikom-db.ac.id

Rahmat Budiarto
College of Computer Science & IT
Albaha University
Saudi Arabia
rahmat@bu.edu.sa

Deris Stiawan
Department of Computer Engineering,
Faculty of Computer Science,
Universitas Sriwijaya, Indonesia
deris@unsri.ac.id

Darmawijoyo Hanapi
Faculty of Mathemathics and Natural Science, Universitas Sriwijaya,
Indonesia
darmawijoyo@yahoo.com

***Abstract*— Internet of Things (IoT) networks operators may not be fully aware whether each IoT device in their network is functioning safe enough from cyber-attacks. This paper develops an IoT traffic dataset with the purpose of of network traffic analytics to characterize IoT devices, including their typical behaviour mode. We set up an IoT environment/testbed consists of several sensors/nodes and uses Zigbee communication protocol to collect and synthesize traffic traces. Normal dataset and anomaly/attack dataset are built using AES technique. We then perform the traffic analysis using key extraction technique. The analysis approach used in this work provides good results in differentiating anomaly from normal traffic.**

Keywords*— Internet of things, zigbee, AES, key extraction, network traffic analysis

I. Introduction

Internet of things (IoT) has become a technology that has its own specific growth in the global development of technology. Currently, more than seven billion of "smart" IoT devices that can autonomously interact with each other and be remotely monitored/controlled are used to assist human at homes, enterprises, campuses and cities, [1][2].

This fast growth of IoT network in scale produces challenge in operational, because it is difficult for the administrator to know what IoT devices are connected and whether they are functioning normally. The lack of visibility into IoT devices can make it very complex for the administrator to trouble-shoot problems in their IoT network infrastructure, and may become particularly disastrous when cybersecurity attacks have breached this critical infrastructure [3].

This paper attempts to address the above problem by characterizing IoT traffic at the network-level, and using this to identify and classify IoT devices, alongside detecting anomalous behavior. The nature of IoT devices are easier to infiltrate [4], thus understanding the nature of IoT traffic is important, and profiling IoT traffic may enhance cyber-security. The huge heterogeneity in IoT devices has led researchers to propose network-level security mechanisms that analyze traffic patterns to identify attacks. The success of the mechanisms relies on a good understanding of what normal IoT traffic profile looks like.

We set up an IoT network environment/tesbed with over 5 IoT devices, comprising different types of sensors. The main contribution of this work is to collect data traces from this environment over a period of several weeks, and to make traces include raw packets (pcap) and flow information, annotated with specific device attributes, providing researchers a rich dataset to investigate many aspects of IoT.

II. Relevant Theories

A. Internet of Things(IoT)

Embedded system devices which supported in terms of connectivity, good mobility, as well as power management resources which more efficient, which currently called with Internet of Things (IoT) [5] [6].

B. Zigbee Protocol

ZigBee is one of the network protocol which is used as a standard protocol of transmitting data. The protocol defined Zigbee Alliance covers Network Layer, Application Layer, and Security Layer, and uses IEEE 802.15.4 standard for the physical layer (PHY and MAC). Zigbee protocol technology has several advantages, its can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones [7], including easy to be implemented in the network, relatively cheap, and flexibility in performing data transmission [8]. An example of architectural topology of Zigbee protocol is shown in Fig. 1.

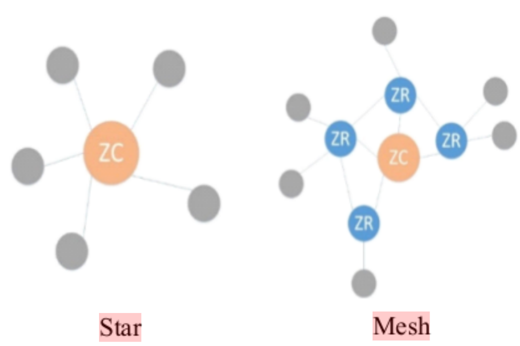

Fig. 1. Example of architectural topology of Zigbee

Table 1 shows the width of frequency and data speed of Zigbee protocol that uses Direct Sequence Spread Spectrum (DSSS) modulation method and Quadratutre Phase Shift Keying (QPSK) modulation type for 2.4 GHz frequency [9].

C. Media access control (MAC)

In this section will describe Media Access Control (MAC).

1) Media access control (MAC) Layer : Media access control (MAC) layer defined by IEEE802.15.4 standard has a task to access the channel going to be used. This layer has two mechanisms: beacon mode that uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique and non-mode beaconthat uses the non CSMA/CA technique [10]. Besides, this layer uses acknowledgement frames, with security data using 128 bit AES encryption and authentication while verification data using CRC 16 bit. Fig. 2 illustrates the MAC Layer super frame diagram.

2) Media access control (MAC) security : Zigbee protocol uses the security services which specified in IEEE802.15.4 standard to secure the frame of Medium Access Control (MAC) layer. MAC layer provides basic monitoring functions and access media wireless communication to coordinate data transmission from higher layers. This layer also provides optional security services, including access control, data encryption, frame integrity, and sequential freshness. The security service is used in various combinations based on one of the 3 security modes supported by IEEE802.15.4 standard, namely the unsecured mode, access control list (ACL) mode and secrured mode.

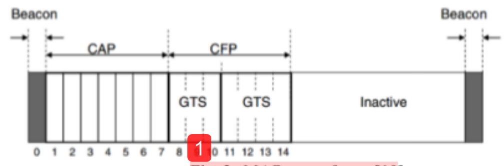

Fig. 2. *MAC super frame* [10]

D. Advanced encryption standard (AES)

The Advanced Encryption Standard algorithm [11] is one of the cryptographic algorithms that implements Rijndeal algorithm. The algorithm is able to encrypt and decrypt data blocks using a length of 128 bits of data and has 128 bits, 192 bits, or 256 bits key locks. The input and Output from AES algorithm consists of a data sequence with a size of 128 bits which then called as data block (plaintext) and then will be encrypted into a ciphertext. Fig. 3 depicts the encryption process.

E. Message integrity code (MIC)

Integrity and freshness of data is one of the main concept of security on ZigBee. In this concept, some secret keys and different security methods are used to ensure the integrity and freshness of a data. Message integrity code (MIC) ensures that the data are not modified while in transit, as illustrated in Fig. 4.

Table I. Frequency width and data speed.

PHY	Frequency Band	Channel Numbering	Speading Parameters		Data Parameters		
			Chip Rate	Modulation	Bit Rate	Symbol Rate	Modulation
868/915 MHz	868-870 MHz	0	300 kchip/s	BPSK	20 kb/s	20 kbaud	BPSK
	902-928 MHz	1 to 10	600 kchip/s	BPSK	40 kb/s	40 kbaud	BPSK
2.4 GHz	2.4-2.4835 GHz	11 to 26	2.0 kchip/s	O-QPSK	250 kb/s	62,5 kbaud	16-ary orthogonal

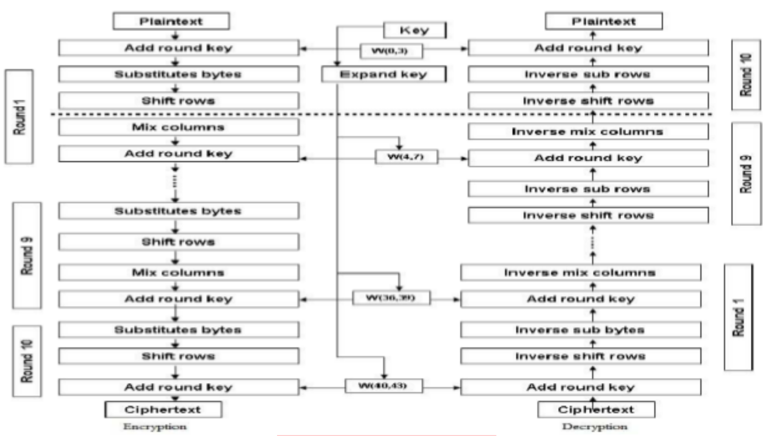

Fig. 3. Encryption Process [11]

III. Experiments

This section describes the experimental set up, data capturing and key extraction. Fig. 5 shows the sequences of research activities.

This research activities have three stages in completion, where at the first stage is conducting literature study related to the research topic. The second stage is designing the topology for the IoT environment by deploying few nodes with sensor installed on each node and using zigbee Protocol as standard for data transmission. The third stage is capturing data by performing two scenarios for normal and anomaly situations. For simplicity, at the moment we focus on 5 nodes with 1 attached sensor each and five minutes interval for data capturing. We repeat the experiments 10 times. The fourth stage is the key extraction process from the captured dataset. Details of stages 2, 3, and 4 are described in the following sub-sections.

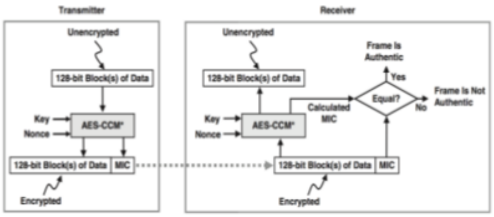

Fig. 4. Message integrity code (MIC) mechanism.

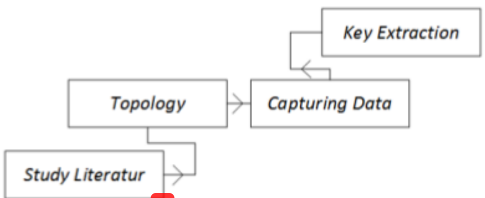

Fig. 5. Research activities sequence.

A. Topology

The experiment environment uses star topology with two protocols, WiFi and Zigbee protocols; Zigbee version one and version two along with their middleware to connecting nodes to the WiFi backbone. Fig. 6 depicts the topology.

In this research is using five sensors on each node, where on each node is attached one sensor for sensing data. The main focus in research is on zigbee protocol version two which become primary object encryption data or the application of the Advanced Encryption Standard (AES) algorithm.

B. Data Capturing

Fig. 6. IoT network environment topology

Data Capturing is conducted for 5 minutes and repeated for 10 times of experiments. Datasets is built for two categories of data, which are normal dataset and anomaly/attack dataset as shown in Table 2 and Table 3. Normal data packets are obtained from regular normal data transmissions while anomaly/attacks data packets are generated by launching a distributed denial of service (Ddos) attack. Both type of data are captured during the same interval capturing time.

Table II. Active encryption data.

Experiment #	Number of packets	Number of ACK packet	Number of frame length	Average of date length	ACK length
Normal dataset of active encryption experiment					
1	257	129	128	51	5
2	446	320	126	51	5
3	457	329	128	51	5
Anomaly/Attack dataset of active encryption experiment					
1	4582	2237	339	65	5
2	3580	1736	1839	45	5
3	5770	2792	2973	50	5

Table III. Non-active encryption data

Experiment #	Number of packets	Number of ACK packet	Number of frame length	Average date length	ACK length
Normal dataset of non-active encryption experiment					
1	695	336	359	43	5
2	626	311	315	43	5
3	649	325	324	43	5
Anomaly/Attack dataset of non-active encryption experiment					
1	3401	1671	1729	70	5
2	4372	2162	2210	38	5
3	3166	1561	1605	50	5

C. Key Extraction

This stage involves steps: datasets conversion, feature extraction, and key extraction. Fig. 7 shows psuedocode extracts the key on the dataset.

Psuedocode Ekstrack

```
Cipher (byte in [4*Nb], byte
out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state [4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
For round = 1 step 1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state,
w[round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state,
w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end
```

Fig. 7. Pseudocode for extraction process

In performing key extraction, a python-based framework KillerBee, a tool set for exploring and exploiting network security Zidbee, as well as IEEE802.15.4 standard are used. One of the KillerBee tool is zbstumbler that sends bacon request frames, captures and displays summary of information about the devices found. The output of the zbstumbler can be inserted into the Comma Separated Value SV) file by using option–*w* in the command and give a name to the file which will be used to store the output, as shown in Fig.8. In this case, the output file is saved as a .csv zigbee.

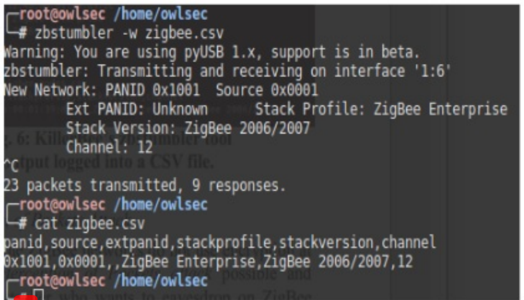

Fig. 8. *Output* from *zbstumbler KillerBee tool is* saved into CSV file

There are many ZigBee networks do not use encryption at all, which causes the attackers are able to misuse information on the devices. Attackers can exploit zbdump KillerBee to capture and store traffic into a captured file. This process is shown in Fig. 9. *-c* option of the command is used to capture traffic on a certain channel. The output file is saved with the name zigbee_node. Dump using *–w* option in the command.

Fig. 9. Zbdump KillerBee captured and saved traffic into capture file

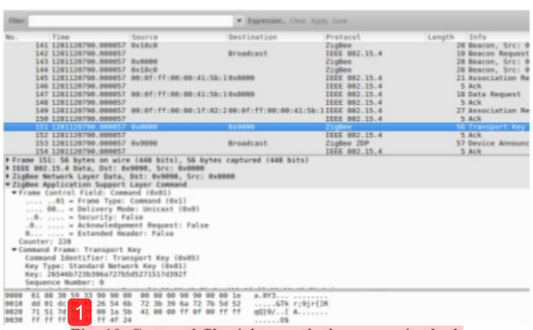

Fig. 10. Captured file zigbee_node.dump on wireshark

When we open the captured file zigbee_node. dump using the Wireshark tool, we obviously can see the key information (See highlighted row in Fig. 10). It means that attackers also easily will be able to see and analyze the captured data/information.

The step now is to analyze the packets of the captured traffic with key extraction. Before doing the extraction, the captured packets which in the form of libpcap file is converted into Daintree Capture files (DCF) file using zbconvert tool. This file format conversion can be done by adding –i option into the zbconvert command to insert the capture file which will be converted (input file), and –o option to save the convert results file (output file). The process of converting the file is illustrated in Fig. 11. In ZigBee protocol, the key extraction process uses zbdsniff tool of KillerBee to find NWK frames and keys. Having done finding the keys, zbdsniff prints the result on the terminal, as shown in Fig. 12.

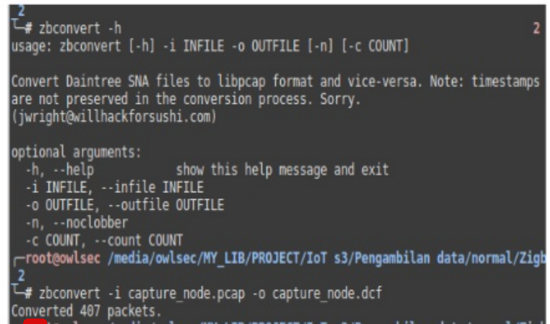

Fig. 11. *Zbconvert* KillerBee converts captured data into DCF format.

Fig. 12 shows that *zbdsniff* tool successfully finds a network key along with the key, the MAC destination, and source addresses. If we compare the information shown in Fig. 10 and Fig. 12, we can conclude that the information obtained by *zbdsniff* tool are the same information obtained by Wireshark tool. Fig. 13 shows the matching correlation between the information in Fig. 10 and Fig. 12.

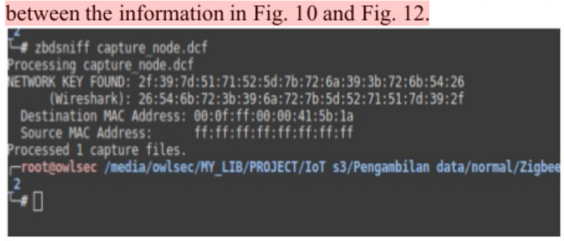

Fig. 12. *Zbdsniff* KillerBee performs the key extraction.

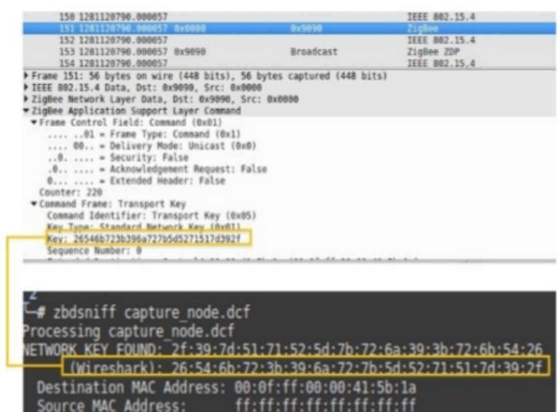

Fig. 13. Matching correlation on information on Wireshark and *zbdsniff*.

Fig. 14 and Fig. 15 shows active encryption before and after entering key, respectively. There are attributes that can be used to differentiate the information from each row of the captured data before and after insertion of the key.

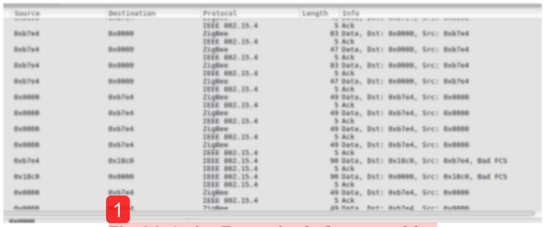

Fig. 14. Active Encryption before entered *key*

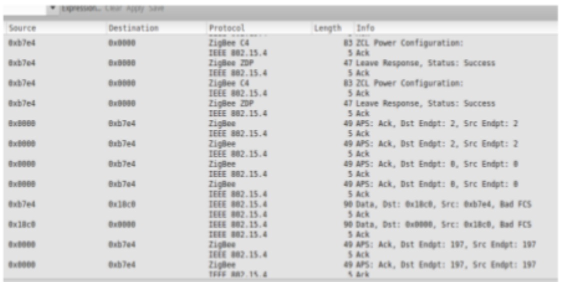

Fig. 15. Active Encryption after entered *key*

IV. CONCLUSION AND FUTURE WORK

In this work, we have built a small scale of datasets (normal traffic and anomaly/attack datasets) from an IoT network environment/ testbed and performed traffic analysis using key extraction. The IoT network environment uses Zigbee protocol and can be easily scale up to capture more complex devices/traffic attributes. The research stages used in this work can be used for profiling IoT devices and networks with the main aim is to strengthen the cyber security.

We expect that the dataset produced in this work lay the foundation for giving more visibility of devices in IoT network, and support future works on IoT network security and performance.

ACKNOWLEDGMENT

This reserach supported by STIKOM Dinamika Bangsa through human resource development programs and collaboration with Comnet Lab Universitas Sriwijaya.

REFERENCES

[1] G. Cerullo, G. Mazzeo, G. Papale, B. Ragucci, and L. Sgaglione, IoT and Sensor Networks Security, 1st ed. Elsevier Inc., 2018.

[2] M. Ammar, G. Russello, and B. Crispo, "Journal of Information Security and Applications Internet of Things :A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018.

[3] A. Sivanathan, D. Sherratt, H.B. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman, Characterizing and Classifying IoT Traffic in Smart Cities and Campuses, Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, USA, 1-4 May 2017, DOI: 10.1109/INFCOMW.2017.8116438.

[4] S. Notra et al., "An Experimental Study of Security and Privacy Risks with Emerging Household Appliances," in Proc. M2MSec, Oct 2014.W. Razouk, G. V Crosby, and A. Sekkaki, "New security approach for ZigBee Weaknesses," *Procedia - Procedia Comput. Sci.*, vol. 37, pp. 376–381, 2014.

[5] T. J. Rao Fang, "Energu consumption research of AES encryption Algorithm in Zegbee," p. 6, 2014.

[6] A. Abane, M. Daoui, S. Bouzefrane, and P. Muhlethaler, "NDN-over-ZigBee : A ZigBee Support for Named Data Networking," *Futur. Gener. Comput. Syst.*, 2017.

[7] K. Cho, S. Lee, B. Kang, K. Jang, and P. Ferrão, "Design and Implementation for Data Protection of Cooling Energy IoT utilizing OTP in the Wireless Mesh Network utilizing OTP in the Mesh Assessing the feasibility of Wireless using the heat Network temperature function for a district heat demand forecast," *Energy Procedia*, vol. 141, pp. 540–544, 2017.

[8] H. Kim, J. Chung, and C. H. Kim, "Secured communication protocol for internetworking ZigBee cluster networks q," *Comput. Commun.*, vol. 32, no. 13–14, pp. 1531–1540, 2009.

[9] O. Olayemi, H. Keijo, M. Asikainen, N. Vidgren, P. Toivanen, Three Practical Attacks Against ZigBee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned, 14th IEEE International Conference on Hybrid Intelligent Systems, Kuwait, Dec. 2014, DOI:10.1109/HIS.2014.7086198.

[10] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks : A survey on the state of the art and the 802 . 15 . 4 and ZigBee standards," vol. 30, pp. 1655–1695, 2007.

[11] L. I. Zhen-rong, Z. Yi-qi, Z. Chao, and J. I. N. Gang, "Low-power and area-optimized VLSI implementation of AES coprocessor for Zigbee system," *J. China Univ. Posts Telecommun.*, vol. 16, no. 3, pp. 89–94, 2009.

978-1-5386-5721-8/18/$31.00 ©2018 IEEE

Monitoring Connectivity of Internet of Things Device on Zigbee Protocol

ORIGINALITY REPORT

93%

SIMILARITY INDEX

PRIMARY SOURCES

1	Benni Purnama, Sharipuddin, Kurniabudi, Rahmat Budiarto, Deris Stiawan, Darmawijoyo Hanapi. "Monitoring Connectivity of Internet of Things Device on Zigbee Protocol", 2018 International Conference on Electrical Engineering and Computer Science (ICECOS), 2018 Crossref	2601 words — 87%
2	www.restorativeacupuncture.com Internet	40 words — 1%
3	docs.zigbee.org Internet	35 words — 1%
4	scholar.ui.ac.id Internet	26 words — 1%
5	Mohamed Shaban, Zeliha Ogur, Ahmed Shalaby, Ali Mahmoud, Mohammed Ghazal, Harpal Sandhu, Henry Kaplan, Ayman El-Baz. "Automated Staging of Diabetic Retinopathy Using a 2D Convolutional Neural Network", 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2018 Crossref	20 words — 1%
6	repository.tudelft.nl Internet	16 words — 1%
7	"Table of Contents", 2018 International Conference on Electrical Engineering and Computer Science (ICECOS), 2018 Crossref	15 words — 1%

8 seminarprojects.net
Internet
14 words — < 1%

9 Herri Setiawan, Jazi Eko, Retantyo Wardoyo, Purwo Santoso. "The Group Decision Support System to Evaluate the ICT Project Performance Using the Hybrid Method of AHP, TOPSIS and Copeland Score", International Journal of Advanced Computer Science and Applications, 2016
Crossref
8 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		