Lecture Notes in Networks and Systems 116

Maitreyee Dutta
C. Rama Krishna
Rakesh Kumar
Mala Kalra *Editors*

Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India

Springer

Lecture Notes in Networks and Systems

Volume 116

Maitreyee Dutta · C. Rama Krishna ·
Rakesh Kumar · Mala Kalra
Editors

Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India

Springer

Editors
Maitreyee Dutta
Department of IMCO
National Institute of Technical Teachers
Training and Research
Chandigarh, India

C. Rama Krishna
Department of CSE
National Institute of Technical Teachers
Training and Research
Chandigarh, India

Rakesh Kumar
Department of CSE
National Institute of Technical Teachers
Training and Research
Chandigarh, India

Mala Kalra
Department of CSE
National Institute of Technical Teachers
Training and Research
Chandigarh, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-15-3019-7 ISBN 978-981-15-3020-3 (eBook)
https://doi.org/10.1007/978-981-15-3020-3

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Committee Members

Patron

Dr. S. S. Pattnaik, Director, National Institute of Technical Teachers Training and Research, Chandigarh, India

Conference Chair(s)

Dr. Maitreyee Dutta, Professor & Head, IMCO, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. C. Rama Krishna, Professor & Head, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India

Conference Coordinator

Dr. Rakesh Kumar, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. Mala Kalra, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India

Proceedings Editors

Dr. Maitreyee Dutta, Professor & Head, IMCO, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. C. Rama Krishna, Professor & Head, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. Rakesh Kumar, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. Mala Kalra, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India

Local Organizing Committee

Dr. Maitreyee Dutta, Professor & Head, IMCO, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. C. Rama Krishna, Professor & Head, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. Rakesh Kumar, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Dr. Mala Kalra, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Ms. Shano Solanki, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Mr. Amit Doegar, Assistant Professor, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
Mr. Amrendra Sharan, Jr. System Programmer, Department of Computer Science & Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India

Student Volunteers

Mr. Talvinder Singh, M.E. Student, National Institute of Technical Teachers Training and Research, Chandigarh, India
Mr. Aaqib, M.E. Student, National Institute of Technical Teachers Training and Research, Chandigarh, India
Ms. Aastha Sood, M.E. Student, National Institute of Technical Teachers Training and Research, Chandigarh, India
Ms. Empreet, M.E. Student, National Institute of Technical Teachers Training and Research, Chandigarh, India
Ms. Nikita Katnoria, M.E. Student, National Institute of Technical Teachers Training and Research, Chandigarh, India
Ms. Savneet Kaur, M.E. Student, National Institute of Technical Teachers Training and Research, Chandigarh, India
Mr. Kamal Deep, Research Scholar, National Institute of Technical Teachers Training and Research, Chandigarh, India
Ms. Manisha Malik, Research Scholar, National Institute of Technical Teachers Training and Research, Chandigarh, India

Preface

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete."

—Buckminster Fuller

It's a great privilege for us to present the proceedings of International Conference on IoT Inclusive Life (ICIIL) 2019 to the authors, delegates and general public. We hope that you will find it useful, exciting and inspiring.

Unlike previous conferences, this time the theme was the link between the IoT and various applications in day-to-day life. The power of Internet connectivity has now stepped beyond computers and smartphones. Every 'smart' device around us is now aiming to solve real-world problems with digital interventions. These are the real-life applications of IoT. Needless to mention, the buzz around IoT is immense. This disruptive technology is penetrating into various industries, developing new real-life applications of IoT and connecting every Internet-enabled device around us. But amongst the mad rush of 'newer' and 'better' IoT applications, some shine through more than the rest.

ICIIL 2019 aimed to provide a platform for discussing the issues, challenges, opportunities and findings in the area of IoT. The ever-changing scope and rapid development of IoT create new problems and questions, resulting in the real needs for sharing brilliant ideas and stimulating good awareness of this important research field.

This book focuses on the following sub-themes:

- Security and Privacy in IoT
- IoT Sensing, Monitoring, Networking and Routing
- Data Science and Computational Intelligence
- IoT Enabling Technologies

The book contains survey papers highlighting the challenges or manuscripts showing simulation or testbed-based experimental results. We hope this book will be quite useful for academicians, researchers and scientists in order to carry out further experimentation and technology enhancements.

Chandigarh, India

Maitreyee Dutta
C. Rama Krishna
Rakesh Kumar
Mala Kalra

Contents

Security and Privacy in IoT

Remotely Triggered Blackhole Routing in SDN for Handling DoS 3
Sugandhi Midha and Khushboo Tripathi

An Improved Authentication and Key Agreement Protocol for Smart Healthcare System in the Context of Internet of Things Using Elliptic Curve Cryptography 11
Uddalak Chatterjee, Dipanwita Sadhukhan and Sangram Ray

Highly Scalable Block Cipher Encryption in MapReduce-Based Distribution System 23
Prashant Verma, Gurjit Singh Walia and Kapil Sharma

RansomAnalysis: The Evolution and Investigation of Android Ransomware 33
Shweta Sharma, Rakesh Kumar and C. Rama Krishna

On the Applicability of Certificateless Public Key Cryptography (CL-PKC) for Securing the Internet of Things (IoT) 43
Manisha Malik, Kamaldeep and Maitreyee Dutta

Performance Evaluation of Advanced Machine Learning Algorithms for Network Intrusion Detection System 51
Sharfuddin Khan, E. Sivaraman and Prasad B. Honnavalli

Low-Light Visible and Infrared Image Fusion in NSST Domain 61
Apoorav Maulik Sharma, Ayush Dogra, Bhawna Goyal, Renu Vig and Sunil Agrawal

Automated Sleep Stage Classification Based on Multiple Channels of Electroencephalographic Signals Using Machine Learning Algorithm 69
Santosh Kumar Satapathy and D. Loganathan

Ontology-Driven Traffic Scenario Modeling for Situational Assessment and Decision-Making at Expressway Toll Plaza 85
Annu Mor and Mukesh Kumar

IoT Sensing, Monitoring, Networking and Routing

Congestion Aware and Stability Based Routing with Cross-Layer Optimization for 6LowPAN 99
Anita Sethi, Sandip Vijay and Vishal Kumar

A Survey on Handover in LTE Heterogeneous Networks 111
Manoj and Sanjeev Kumar

Two-Level Data Dissemination for Energy-Efficient Routing in IoT-Based Wireless Sensor Network 127
Roopali Dogra, Shalli Rani and Bhisham Sharma

A Comparative Study of Cluster-Head Selection Algorithms in VANET 143
Poonam Thakur and Anita Ganpati

Health Monitoring Multifunction Band Using IOT 159
Pooja Nagpal and Sarika Chaudhary

Particulate Matter Assessment in Association with Temperature and Humidity: An Experimental Study on Residential Environment . . . 167
Jagriti Saini, Maitreyee Dutta and Gonçalo Marques

Comparative Study of Ambient Air Quality Prediction System Using Machine Learning to Predict Air Quality in Smart City 175
Gopal Sakarkar, Sofia Pillai, C. V. Rao, Atharva Peshkar and Shreyas Malewar

A Configurable Healthcare Monitoring System 183
Gurdip Singh, Shravanthi Kallem and Pavani Ayyagari

Evaluation of Hand Movement Using IoT-Based Goniometric Data Acquisition Glove 193
Prashant Jindal, Rashi Aditi Ranjan, Poojita Garg, Pranav Raj, Parneet Kaur, Varun Karan, Ishan Madhav and Mamta Juneja

CoTusk: IoT-Based Tooth Shade Detecting Device 201
Mamta Juneja, Jannat Chawla, Sumindar Kaur Saini, Divya Bajaj and Prashant Jindal

Data Science and Computational Intelligence

Multi-agent Based Recommender System for Netflix 211
Harjot Kaur, Harsharandeep Kaur and Amitpal Singh

Review of Various Sentiment Analysis Approaches 223
Ishana Attri and Maitreyee Dutta

Hyperparameter Tuning and Optimization in Machine Learning for Species Identification System 235
Sofia K. Pillai, M. M. Raghuwanshi and M. Gaikwad

Major Convolutional Neural Networks in Image Classification: A Survey 243
Navdeep Kumar, Nirmal Kaur and Deepti Gupta

Prediction of Accuracy of High-Strength Concrete Using Data Mining Technique: A Review 259
Aman Kumar and Navdeep Mor

AntMiner: Bridging the Gap Between Data Mining Classification Rule Discovery and Bio-Inspired Algorithms 269
Bhawna Jyoti and Aman Kumar Sharma

Fuzzy K-Medoid Clustering Strategy for Heterogeneous and Dynamic Data for IoT Scenario 279
Priya Dogra and Rakesh Kumar

Leaf Disease Detection and Classification: A Comprehensive Survey 291
Manpreet Kaur and Rekha Bhatia

Performance Evaluation of Different Classification Factors for Early Diagnosis of Alzheimer's Disease 305
Agha Alfi Mirza, Maitreyee Dutta, Siddheshwari Mishra and Agha Urfi Mirza

Real-Time Multi-cue Object Tracking: Benchmark 317
Ashish Kumar, Gurjit Singh Walia and Kapil Sharma

IoT Enabling Technologies

IoT-Driven Real-Time Monitoring of Air Pollution with Dynamic Google Mapping 327
Nikhil and Milanpreet Kaur

Android Things: A Comprehensive Solution from Things to Smart Display and Speaker 339
Rohit Roy, Sayantika Dutta, Sagnick Biswas and Jyoti Sekhar Banerjee

Energy-Aware VM Migration in Cloud Computing 353
Shashi Bhushan Singh Yadav and Mala Kalra

Deadline Constrained Energy-Efficient Workflow Scheduling Heuristic for Cloud 365
Shalu Saharawat and Mala Kalra

Homodyne Detection in WDM FSO System—A Better Solution to Mitigate Scintillation Effects 383
Neha Rani, Preeti Singh and Pardeep Kaur

SSCCJ: System for Source to Source Conversion from C++ to Java for Efficient Computing in IoT Era 393
Preeti Bhatt, Harmunish Taneja and Kavita Taneja

Efficient VM Migration Policy in Cloud Computing Environment 401
Annie Pathania, Kiranbir Kaur and Prabhsimran Singh

Software-Defined Networks: Need of Emerging Networks and Technologies 411
Deepak Kumar and Jawahar Thakur

Learning Rich Features from Software-as-a-Service Cloud Computing for Detecting Trust Violations 445
Mahreen Saleem, M. R. Warsi and Saiful Islam

Improved Symbiotic Organism Search Based Approach for Scheduling Jobs in Cloud 455
Deepika Srivastava and Mala Kalra

About the Editors

Dr. Maitreyee Dutta completed her basic studies in ECE at Guahati University in 1993; her M.E. at PEC Chandigarh in 1999; and her Ph.D. at Punjab University in 2007. She joined the NITTTR Chandigarh in 2001. She is currently a Professor and Head of the institute's IMCO Unit. She has secured funding for two major projects from the Ministry of IT, New Delhi, and Ministry of Social Justice. She received the Rota Women's Distinction Award from the Rotary Club Chandigarh Midtown in 2013, and the Best Teacher Award from Bharatiya Shikshan Mandal, Uttar Pradesh, in the same year.

Dr. C. Rama Krishna completed his B.Tech. at the JNTU, Hyderabad; his M.Tech. at CUSAT, Cochin; and his Ph.D. at the IIT, Kharagpur, in the area of MANET. He is a Senior Member of the IEEE, USA. Since 1996, he has been working with the Department of CSE, NITTTR, Chandigarh, and currently holds the position of Professor and Head of Department, with more than 22 years of teaching experience. He has more than 100 research publications in international and national journals and conference proceedings to his credit, has implemented several projects funded by various government and private agencies in India, and holds one patent.

Dr. Rakesh Kumar received his B.Tech. in CSE from the IKGPTU, Jalandhar; his M.Tech. in IT from the GGSIPU, New Delhi; and his Ph.D. in Computer Engineering from the NIT Kurukshetra in 2004, 2008, and 2015, respectively. With more than 15 years of teaching experience, he is currently working as an Assistant Professor at the Department of CSE, NITTTR Chandigarh. He has several international/national conference/journal publications to his credit, and serves as a reviewer for many international journals/conferences.

Dr. Mala Kalra is an Assistant Professor at the Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research (NITTTR), Chandigarh, India. She received her B.E. in Computer Science and Engineering from the MDU, Rohtak, India, in 2001; her M.E. in CSE from PEC

University of Technology, Chandigarh, India, in 2006; and her Ph.D. in CSE from the PU, Chandigarh, in 2019. She has more than 15 years of teaching and research experience, and has published over 40 research papers in reputed international journals and conference proceedings.

Security and Privacy in IoT

Remotely Triggered Blackhole Routing in SDN for Handling DoS

Sugandhi Midha and Khushboo Tripathi

Abstract The DoS attack is one of the simplest yet most vulnerable attacks that is prominent in SDN. No doubt, SDN is leveraging several benefits like no vendor lock-ins, better fault tolerance, more opportune to innovations, etc., over traditional networks. Yet, SDN controller is a bigger target of security attacks. DoS makes the SDN controller unavailable for providing information/services. Remotely Triggered Black Hole technique is used to protect SDN from DoS attack. This technique has the ability to drop traffic coming from an undesired network element before it penetrates into the network. Our paper explains how this algorithm works and how it can be used to secure our SDN. We have tried to analyse, quantify and detect the impact of DoS in SDN. One key advantage of the proposed approach is its ability to accurately detect DoS with a nominal rate of failure. We simulated the system with our test bed of virtual machine with different attack scripted in Python.

Keywords Denial of Service (DoS) · Software-defined network controller · Remotely Triggered Black Hole (RTBH) routing · Access Control List (ACL)

1 Introduction

Software-Based Network [1] commonly called Software-Defined Network (SDN) is a new networking technology that has removed several shortcomings like high equipment cost, buggy product, complex infrastructure, vendor dependencies, etc., of a conventional network. SDN has made innovations easy and has brought flexibility in the networking environment. SDN has lowered down the cost and reduced the complexity of network devices.

SDN is broken down into three layers: Application Plane, Control Plane and Data Plane.

Application plane is how the user manages and uses applications like security, load balancing, SNMP, NETCONF, etc. Control Plane defines how SDN Controller

S. Midha (✉) · K. Tripathi
Amity University, Gurgaon, India
e-mail: mailmetech@gmail.com

M. Dutta et al. (eds.), *Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India*, Lecture Notes in Networks and Systems 116,
https://doi.org/10.1007/978-981-15-3020-3_1

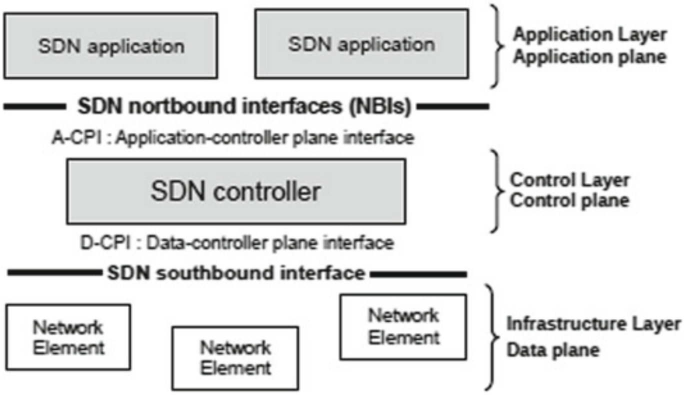


Fig. 1 SDN architecture [2]

handles the Network Elements (NEs). It dynamically provisions the NEs by setting up the flow rules on them. It improves automation by using common APIs and provides a mechanism for the rapid deployment of new services [1]. The Data Plane is merely a collection of physical devices that are responsible for the flow of packets among NEs (Fig. 1).

SDN is the sum of North Bound Interfaces (NBI) and South Bound Interfaces (SBI) which allows the creation of a powerful and dynamic virtual network that enables SDN Controller to configure NEs flow table and allows for more sophisticated traffic management [3].

2 DoS Attack

“**CIA** Triad” [1] is a key term in the security field which refers to three major goals of security:

Confidentiality: It deals with ensuring the privacy and secrecy of information, i.e. no unauthorised user gets access to information and resources.

Integrity: It ensures that no tampering has been done on the data either on the storage or communication medium.

Availability: It ensures that information is available to the intended/right user, i.e. the user is legitimate and has the right to access that information. Ensuring timely information to the legitimate user is the key goal of availability.

DoS is one of the key attacks on the SDN Controller that affects the availability of information to legitimate users. In the DoS attack, a malicious attacker consumes all the network capacity by flooding packets on SDN Controller that attacked SDN Controller is left with no capacity to reply to the legitimate user (Fig. 2).

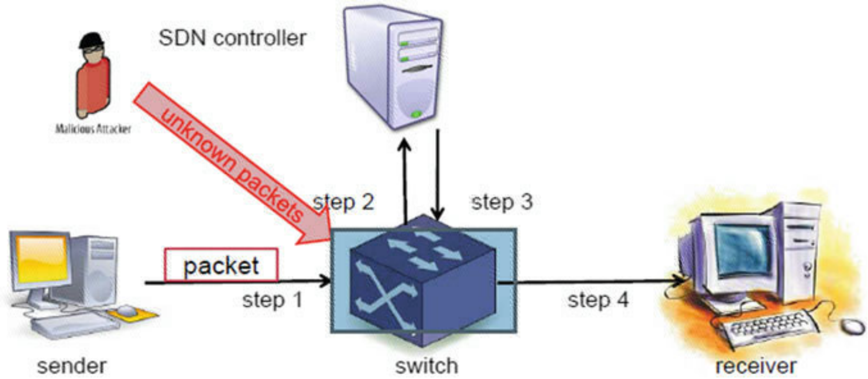


Fig. 2 DoS attack [5]

3 Remotely Triggered Blackhole Routing—Proposed Work

In this paper, the RTBH routing protocol has been proposed for SDN Controller with an aim that all packets from the malicious attacker will be dropped in no time by maintaining ACL (Access Control List). Both of these mechanisms, RTBH routing and ACL, can be applied as an edge on the SDN Controller for providing access to legitimate users. For defeating the DoS attack, SDN Controller can scale up to a level based on the size of ACL. It depends on how quickly a packet is accessed and filtered so that it can either be dropped or forwarded (Fig. 3).

RTBH routing algorithm triggers a discard route and maintains an ACL. ACL is updated from time to time to take care of the scalability issue too. The attacker ID is checked against an ACL. If the ID is not found in ACL, traffic is routed to discard

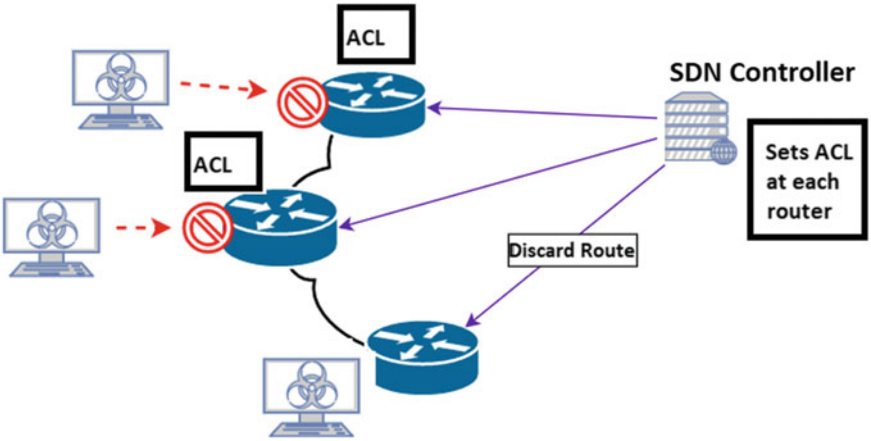


Fig. 3 Maintaining ACL and configuring discard route

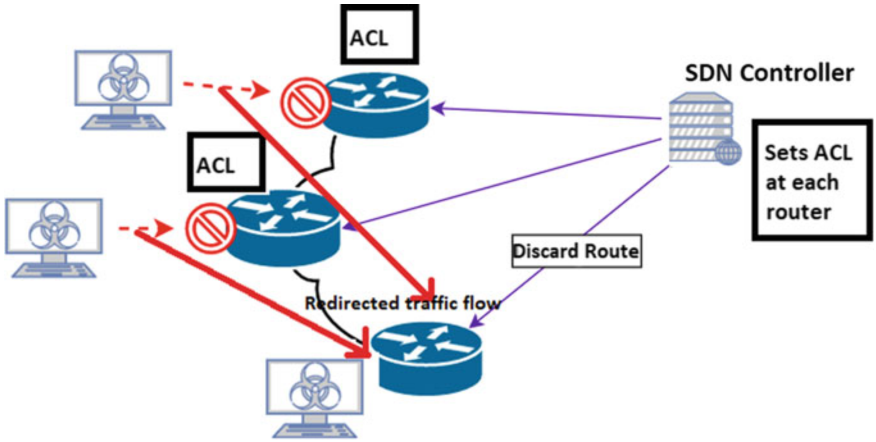
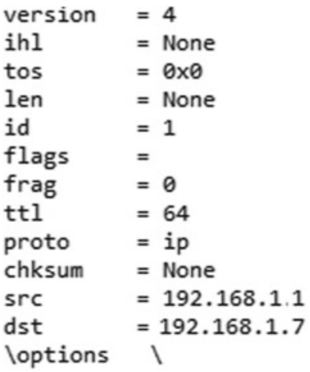


Fig. 4 Redirecting traffic to discard route

the route or else an entry is further checked into the flow table for forwarding the packet to a legitimate user (Fig. 4).

4 Analysis, Detecting and Quantifying DoS—Results and Discussion

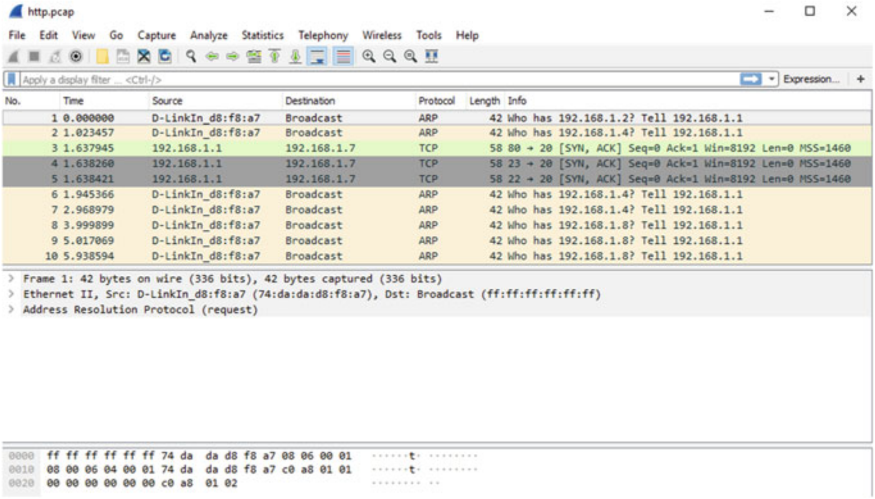
A complete scenario is simulated on the virtual machine using a Python script. IP/TCP stack is used and the src—192.168.1.1 and destination 192.168.1.7 are the valid addresses.



```
version    = 4
ihl        = None
tos        = 0x0
len        = None
id         = 1
flags      =
frag       = 0
ttl        = 64
proto      = ip
chksum     = None
src        = 192.168.1.1
dst        = 192.168.1.7
\options    \
```

Figure 5 shows the Wireshark packet capture file at normal packet flow.

An attacker with the src—192.168.1.6 tries to flood the route with the packets so that legitimate user and controller do not connect.

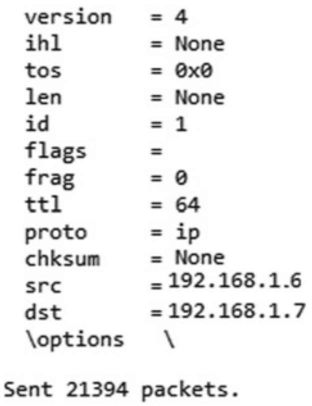


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
2	1.023457	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
3	1.637945	192.168.1.1	192.168.1.7	TCP	58	80 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
4	1.638260	192.168.1.1	192.168.1.7	TCP	58	23 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
5	1.638421	192.168.1.1	192.168.1.7	TCP	58	22 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
6	1.945366	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
7	2.968979	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
8	3.999899	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
9	5.017069	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
10	5.938594	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: D-LinkIn_d8:f8:a7 (74:da:da:d8:f8:a7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 74 da  da d8 f8 a7 08 06 00 01   ······t· ········
0010  08 00 06 04 00 01 74 da  da d8 f8 a7 c0 a8 01 01   ······t· ········
0020  00 00 00 00 00 00 c0 a8  01 02                     ········ ··
```

Fig. 5 Packet capture—normal flow



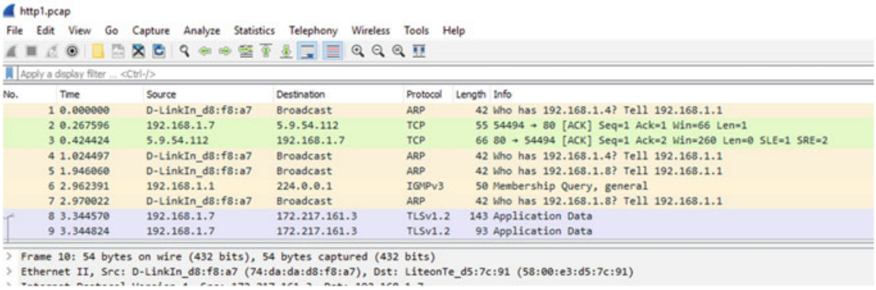
```
version    = 4
ihl        = None
tos        = 0x0
len        = None
id         = 1
flags      =
frag       = 0
ttl        = 64
proto      = ip
chksum     = None
src        =192.168.1.6
dst        =192.168.1.7
\options    \

Sent 21394 packets.
```

Figure 6 shows the Wireshark packet capture file at abrupt packet flow which identifies the source attacker and reroutes the packets to a configured discarded route.

5 Conclusion and Future Work

In this paper, we have discussed what a DoS attack is and what aims to consume network resources and hampers its performance. We highlighted the ways how it could be detected and analysed. We pointed out that in SDN, the control plane is at stake in the case of DoS. We mentioned and focused on Black Hole based routing


http1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
2	0.267596	192.168.1.7	5.9.54.112	TCP	55	54494 → 80 [ACK] Seq=1 Ack=1 Win=66 Len=1
3	0.424424	5.9.54.112	192.168.1.7	TCP	66	80 → 54494 [ACK] Seq=1 Ack=2 Win=260 Len=0 SLE=1 SRE=2
4	1.024497	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.1
5	1.946060	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
6	2.962391	192.168.1.1	224.0.0.1	IGMPv3	50	Membership Query, general
7	2.970022	D-LinkIn_d8:f8:a7	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
8	3.344570	192.168.1.7	172.217.161.3	TLSv1.2	143	Application Data
9	3.344824	192.168.1.7	172.217.161.3	TLSv1.2	93	Application Data

```
> Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: D-LinkIn_d8:f8:a7 (74:da:da:d8:f8:a7), Dst: LiteonTe_d5:7c:91 (58:00:e3:d5:7c:91)
```

Fig. 6 Packet captures—DoS (Packets flooding)

which can serve as an edge to protect our SDN from DoS. No doubt, this routing technique maintains an ACL and there is a serious check on scalability.

For future work, there are many directions to explore to deal with the scalability issue. Our next set of experiments regarding this is in progress.

References

1. A. Owokade, How to configure remotely triggered black hole routing to protect from DDOS attacks (2017), https://sdn.ieee.org/newsletter/January-2016/sdn-in-the-cable-access-network
2. Open Networking Foundation, Software-defined networking: the new norm for networks. White Paper (2012), https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf, pp. xvii, 14, 15, 53, 54
3. A. Mirchev, Survey of concepts for QoS improvements via SDN, in *Seminars FI/ IITM SS 15, Network Architectures and Services* (2015)
4. S. Hassas Yeganeh, Y. Ganjali, Kandoo: a framework for efficicient and scalable offloading of control applications, in *Proceedings of the first workshop on hot topics in software defined networks, HotSDN'12*, (New York, NY, USA), pp. 19–24; (ACM, 2012), pp. xvii, 16, 17
5. AdmelaJukan, Marcel Caria, Siquan Zhao, "Security in SDN", in proceedings of IEEE conference in IEEE, 2014
6. R. Sherwood, M. Chan, A. Covington, G. Gibb, M. Flajslik, N. Handigol, T.-Y. Huang, P. Kazemian, M. Kobayashi, J. Naous, S. Seetharaman, D. Underhill, T. Yabe, K.-K. Yap, Y. Yiakoumis, H. Zeng, G. Appenzeller, R. Johari, N. McKeown, G. Parulkar, Carving research slices out of your production networks with open ow. SIGCOMM Comput. Commun. Rev. **40**, 129, 130 (2010), xvii, 31, 32, 39
7. Open Networking Foundation, OpenFlow, White Paper, https://www.opennetworking.org/wp-content/uploads/…/openflow-switch-v1.5.1.pdf
8. J. Suh, H.-G. Choi, W. Yoon, T. You, T. Kwon, Y. Choi, Implementation of content-oriented networking architecture (CONA): a focus on DDoS countermeasure, in *1st European NetFPGA Developers Workshop* (2010), p. 34
9. R. Sherwood, G. Gibb, K.K. Yap, G. Appenzeller, M. Casado, N. McKeown, G. Parulkar, Flowvisor: a network virtualization layer. OpenFlow Switch Consortium, Technical report (2009)
10. Q. Yan, F. Richard Yu, Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Commun. Mag. (2015)

11. K. Govindarajan, K.C. Meng, H. Ong, A literature review on software-defined networking (SDN) research topics, challenges and solutions, in *IEEE fifth international conference on advanced computing (ICoAC)* (2013)
12. A. Hakiri, A. Gokhalec, P. Berthou, D.C. Schmidtc, T. Gayraud, Software-defined networking: challenges and research opportunities for future internet. **75**(Part A), 453–471 (2014). Elsevier
13. D. Kerutz, P. Essteves, S. Azodolmolky, Software defined networking: a comprehensive survey. Proc. IEEE **103**(1) (2015)
14. A. Kucminski, A. Al-Jawad, P. Shah, R. Trestian, QoS-based routing over software defined networks, in *IEEE international symposium on broadband multimedia systems and broadcasting (BMSB)* (2017)
15. S. Pisharody, J. Natarajan, A. Chowdhary, A. Alshalan, A security policy analysis framework for distributed SDN-based cloud environments. IEEE Trans. Dependable Secur. Comput. **PP**(99) (2017)
16. I. Ahmad, S. Namal, M. Ylianttila, A. Gurtov, Analysis of deployment challenges of host identity potocol (IEEE, 2017)
17. Noxrep, POX: OpenFlow Controller (2015), https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software_Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf
18. Hengky Hank Susanto, Sing Lab, Introduction to SDN, www.cse.ust.hk/~kaichen/courses/spring2015/comp6611/…/SDN-presentation.pptx
19. B. Heller, N. Handigol, V. Jeyakumar, N. McKeown, D. Mazières, Where is the debugger for mySoftware-Defined Network? In *HotSDN* (2012)
20. Z. Hu, M. Wang, X. YAN, Y. YIN, A comprehensive security architecture for SDN, in *The IEEE proceedings of 18th international conference on Intelligence in Next Generation Networks* (IEEE, 2015)
21. S. Shin, G. Gu, Attacking software-defined networks: a first feasibilitystudy, in *Proceedings of the second ACM SIGCOMM workshopon Hot topics in software defined networking* (ACM, 2013), pp. 165–166
22. E. Al-Shaer, S. Al-Haj, Flowchecker: configuration analysis and verification of federated openflow infrastructures. in *Proceedings of the 3rd ACM workshop on assurable and usable security Configuration* (2010)
23. P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, G. Gu, A security enforcement kernel for OpenFlow networks, in *Proceedings of the first workshop on Hot topics in software defined networks* (ACM, 2012), pp. 121–126
24. S. Shin, G. Gu, CloudWatcher: network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?), in *20th IEEE international conference on network protocols (ICNP)*. (IEEE, 2012), pp. 1–6
25. D. Kordalewski, R. Robere, A dynamic algorithmfor loop detection in software defined networks (2012)
26. A. Khurshid, W. Zhou, M. Caesar, P. Godfrey, Veriflow: verifying network-wide invariants in realtime. ACM SIGCOMM Comput. Commun. Rev. **42**(4), 467–472 (2012)
27. H. Yang, S.S. Lam, Real-time verification of networkproperties using atomic predicates, in *ICNP, The IEEE international conference on network protocols* (2013)
28. Z. Hu, J. Luo, Cracking network monitoring inDCNs with SDN, in *2015 IEEE conference on computercommunications, INFOCOM 2015* (Hong Kong, China, 2015), pp. 199–207
29. F. Chen, B. Bruhadeshwar, A.X. Liu, Privacypreservingcross-domain network reachability quantification, in *2011 19th IEEE international conference on network protocols (ICNP)* (IEEE, 2011), pp. 155–164
30. M.J. Freedman, K. Nissim, B. Pinkas, Efficientprivate matching and set intersection, in *Advances in Cryptology-EUROCRYPT 2004* (Springer, Berlin, 2004), pp. 1–19
31. N. Chellani, P. Tejpal, P. Hari, V. Neeralike, Enhancing security in openflow, in *IEEE Proceedings* (2016)
32. O.I. Abdullaziz, Y.-J. Chen, L.-C. Wang, Lightweight authentication mechanism for software defined network using information hiding (IEEE, 2016)

33. S.M. Mousavi, M. St-Hilarie, Early detection of DDoS attacks against SDN controllers (EEE, 2015)
34. IBM Knowledge Center, An overview of the SSL or TLS handshake (2017), http://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm. Accessed 7 Feb 2017

An Improved Authentication and Key Agreement Protocol for Smart Healthcare System in the Context of Internet of Things Using Elliptic Curve Cryptography

Uddalak Chatterjee, Dipanwita Sadhukhan and Sangram Ray

Abstract Internet of Things (IoT) is heterogeneous in nature and has diverse application areas. Smart healthcare (s-health) is one of the most significant applications of IoT that handles sensitive health-related data, which can be manipulated to cause fatal safety consequences. Hence, security and privacy must be considered as the most important factors during the design of wearable s-health. Therefore, it is necessary to establish a secure communication channel between wearable sensors or devices and the remote server of the IoT network. In this work, we propose a protocol for authentication and key agreement using ECC (Elliptic Curve Cryptography) to protect the health-related data in s-health. In this work, trusted sensors take the responsibility of completing the complex cryptographic operations on behalf of resource-constraint sensors. The smartphones accelerometers data and the data received from sensors installed on the body are used to do the trust verification by finding data correlations. Moreover, through security and performance analysis we have shown that the proposed protocol is secure against all relevant cryptographic attacks and is lightweight due to the use of ECC.

Keywords Internet of things · Mutual authentication · Key management · Resource-constrained sensors · ECC (Elliptic curve cryptography) · Body area networks

U. Chatterjee · D. Sadhukhan (✉) · S. Ray
Department of Computer Science and Engineering, National Institute of Technology Sikkim, Ravangla 737139, Sikkim, India
e-mail: dipanwitasadhukhan2012@gmail.com

U. Chatterjee
e-mail: uddalak.udi@gmail.com

S. Ray
e-mail: sangram.ism@gmail.com

M. Dutta et al. (eds.), *Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India*, Lecture Notes in Networks and Systems 116,
https://doi.org/10.1007/978-981-15-3020-3_2

1 Introduction

Importance and issues of s-health: IoT integrates physical objects irrespective of their resource and computing capabilities or type of networks [1] for seamless communication and transmission of data over the Internet. It involves devices with various sensing, measuring and data capture capability sensors, RFID, etc., to achieve intelligent identification and monitoring. One of such standalone IoT device is smart wearable devices that have become an essential part of our daily life. These have a wide area of implementation such as healthcare applications, smart home applications, sports and fitness tracking applications, etc. Wearable devices like Fitbit, smartwatches, etc., in health care have become very common in the present life. The main issues that arise in this context and considered in this paper are – *(i)* how the remote server and the resource-constrained sensors are authenticating each other to be paired; and *(ii)* how to balance users' privacy and usability. Moreover, the sensor nodes have very less computing capabilities and constrained resources in the area of the potential of processing, memory, communication bandwidth, and energy especially in s-health. Since the sensors are of different resource types in nature, the same encryption technique cannot be used for all sensors. Hence, security measures must be pre-embedded. To achieve high-security strength, it is necessary to establish secure key management among the communicating parties. In general, the symmetric encryption algorithms such as AES are well suited to achieve sound security of constraint resources with processing capability. However, due to the high communication overhead and huge storage requirements, the symmetric key encryption techniques are not suitable for this purpose [2]. Asymmetric key cryptography has also its own demerits like high computation and communication overheads which are the prime concern for sensors with less resource and computing capability. Other established security measures also could not be applied due to less resources, low computing capability, and heterogeneity of sensors implanted or worn in the body in IoT-based healthcare system. To prevent sensitive health data from malicious activity, end-to-end (E2E) data protection is crucial.

Our contribution: In this paper, the complex cryptographic operations which need high computing capability and resources are offloaded from less resourceful sensors to resource-rich correlated sensor nodes. Thus, we have proposed an enhanced and lightweight protocol using ECC for s-health in the context of IoT.

Organization of the paper: The structure of the rest of the paper is as follows. Section 2 highlights the summary of the related works; Sect. 3 describes the assumptions and preliminaries for selection; Sect. 4 describes the proposed key establishment protocol; Sect. 5 focuses on the security evaluations of the proposed protocol; Sect. 6 illustrates performance analysis, and finally Sect. 7 concludes the work with an overview of future work directions.

2 Related Work

Authentication and key agreement protocols are mainly motivated to design for establishing a secure key between the communicating entities for secure data transfer as well as to achieve the primitive security objectives such as protection of users privacy or confidentiality of the users credentials that are transmitted over the network; maintain the integrity of the transferred message as well as providing required services to be availed by the legitimate user.

Many different security measures for providing security in IoT devices and other remote servers, in the network have been proposed and implemented to achieve secure authentication between endpoints of the network. Among them, many have proposed public-key cryptography, but could not become successful due to significant computational and processing overheads. Therefore, researchers are aiming to reduce overheads which occur during key agreement and authentication handshake. In the case of resource-constraint sensors, the use of public-key cryptography in such a scenario will increase the overhead since the resources are limited. In [3], the authors have implemented an authentication scheme which is a two-way scheme for the IoT using PKI. X.509 certificates and RSA public keys with DTLS handshake are being used in this approach, which is not suitable as it generates a high amount of network traffic. Other existing protocols using compression of IPV6 header, extension headers, and UDP (User Datagram Protocol) header have been proposed which is standard in 6LoWPAN. To authenticate header and encapsulating security, 6LoWPAN compressions have been presented by the authors in [1] for IPsec payload header. In another interesting approach, the authors in [4] proposed a solution based on the proxy to move the heavy cryptographic operations from a less resourceful device to resource-rich sensor nodes. Although the authors [1] assumed the assisting nodes to be trustworthy, the authors have not described any trust determination technique. Moreover, in the scheme [1] the re-keying processes of compromised proxies are not described, which behaves irrationally or does not perform their assigned task. (n, k) threshold scheme and polynomial interpolation by Lagrange for reconstituting the sender's Diffie–Hellman's public key are considered in these protocols [1, 4] where reconstructing sender's DH public-key k polynomial shares are sufficient. However, the potential threat of revealing the secret key could not be avoided as they [1, 4] have overlooked the threat of revealing these secret keys through cryptanalysis although the shared symmetric keys are considered secure from brute force attacks. The requirement of IoT-based application is to have a secure end-to-end connection between devices. Both the remote server and resource-constrained sensor require having a secure E2E communication link between them that means both ends first need to authenticate each other and securely establish a secret session key to encrypt the transmitted data. In this regard in [2] Diffie–Hellman (DH) security protocol is used in their proposed key agreement and distribution protocol. The security of this key scheme lies in the difficulty of computing discrete algorithms that is very hard to break and also achieves the perfect forward secrecy property. DH key establishment protocol requires both ends to agree first on the appropriate prime (p) and generator (g) numbers. If remote server A wants to communicate with a highly resource-constrained sensor, an E2E key distribution protocol is needed to establish a secure channel between them for further communications. In accordance with this paper [2] the public keys for node B will be generated in server side and eventually the session key will be generated using the DH algorithm. In this research, an enhanced version of the protocol developed in [2] with the same network model explained in [2] is proposed with much lesser communication and computation overheads. The proposed scheme also reduced the existing limitations of the previous protocol [2].

3 Preliminaries

The essential preliminaries for the proposed protocol are discussed as follows:

A. *Finding correlation and selection of assisting sensor nodes*

The sensor nodes have a triaxial accelerometer which is the same as the smartphone to compare data directly for correlation. Accelerometers detect force acting in the opposite direction to the displacement vector. The magnitude of these three axes of accelerometers is used for data correlation. We can get the rate of change of speed over time for a particular sensor. We can find how two signals correlate in the frequency domain by finding coherence, which is the cross-spectral density of each individual signal [2]. After the correlation is found, the selection of assisting trusted sensors in the proximity of the resource-constraint sensor node is done by finding whether they are installed on the body or not. If any of the sensor nodes data is not correlated with the gateway nodes accelerometer's data, then it implies that the sensor is not trusted and therefore could not be assigned any task related to key agreement mechanism.

B. *Network Model*

The network model for the s-health system consists of different sensors with different resource limitations. They are accompanied by triaxial accelerometers which are wearable or implanted on the body of a person and a smartphone working as a gateway. The implanted or wearable sensors are highly resource constraint, therefore they are unable to perform cryptographic operations. Some sensors which are less resource-constraint are able to do heavy cryptographic computations for the key agreement protocol. Others are the devices or sensors with no constraint on resources like remote servers. Now if the remote server wants to communicate with a highly resource-constraint sensor then an E2E key distribution protocol is essential to establish a secure channel for further communications. In this regard, the resource-constraint sensor offloads its heavy computational task to the neighboring trusted sensors which are installed on the body and are correlated.

C. *Elliptic Curve Cryptography (ECC)*

The elliptic curve cryptosystem [5, 6] was initially proposed by Koblitz [7] and then Miller [8] in 1985 to design public-key cryptosystem and presently, it becomes an integral part of the modern cryptography. Let E/F_p denotes an elliptic curve E over a prime finite field F_p, can be defined by the following equation:

$$Y^2 = x^3 + ax + b, \tag{1}$$

where a, $b \in F_p$ and the discriminate D such that, $D = 4a^3 + 27b^2 \neq 0$.

The points on E/F_p together with an extra point O called the point at infinity used for additive identity form an additive group A as

$$A = \{(x, y) : x, y \in Fp, E(x, y) = 0\}u\{0\} \tag{2}$$

Let the order of A be n, which is very large and it can be defined as $n \times G\ mod\ q = O$, where G is the generator of A.

The A be a cyclic additive group under the point addition "+" defined as follows:

$$P + O = P$$

where $P \in A$. The scalar point multiplication over A can be defined as

$$tP = P + P + \ldots P\ (t\ times) \tag{3}$$

The hardness of ECC depends on solving the computational problems of ECC such as ECDLP in polynomial time.

4 Proposed Authentication and Key Agreement Protocol

In our approach, if a remote server R_s wants to communicate with resource-constraint node the gateway reports the *IDs* of neighboring assisting nodes installed on the body by the data correlation process [2]. The sensor is said to be compromised when the neighboring sensor accelerometer's data and gateway accelerometer's data fails to correlate. The asymmetric key agreement involves heavy cryptographic computations. Since the node R_{c_s} is resource constraint it distributes the heavy tasks to its neighboring trusted sensors installed on the body for assistance. In our proposed protocol for key agreement and distribution, ECC-based Diffie–Hellman (ECDH) protocol is used since ECC based scheme is much lighter and secure than the DH method [9–12, 15–19]. The proposed key agreement protocol is designed considering the following initial assumptions (Table 1).