Lecture Notes on Data Engineering
and Communications Technologies 55

P. Karuppusamy
Isidoros Perikos
Fuqian Shi
Tu N. Nguyen *Editors*

Sustainable Communication Networks and Application

Proceedings of ICSCN 2020

Springer

Lecture Notes on Data Engineering and Communications Technologies

Volume 55

The aim of the book series is to present cutting edge engineering approaches to data technologies and communications. It will publish latest advances on the engineering task of building and deploying distributed, scalable and reliable data infrastructures and communication systems.

The series will have a prominent applied focus on data technologies and communications with aim to promote the bridging from fundamental research on data science and networking to data engineering and communications that lead to industry products, business knowledge and standardisation.

Indexed by SCOPUS, INSPEC.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at http://www.springer.com/series/15362

P. Karuppusamy · Isidoros Perikos ·
Fuqian Shi · Tu N. Nguyen
Editors

Sustainable Communication Networks and Application

Proceedings of ICSCN 2020

Springer

Editors
P. Karuppusamy
Department of EEE
Shree Venkateshwara Hi-Tech Engineering
Erode, Tamil Nadu, India

Fuqian Shi
College of Information and Engineering
Wenzhou Medical University
Wenzhou, China

Isidoros Perikos
Department of Computer Engineering
and Informatics
University of Patras
Patras, Greece

Tu N. Nguyen
Department of Computer Science
Purdue University Fort Wayne
Fort Wayne, IN, USA

ISSN 2367-4512 ISSN 2367-4520 (electronic)
Lecture Notes on Data Engineering and Communications Technologies
ISBN 978-981-15-8676-7 ISBN 978-981-15-8677-4 (eBook)
https://doi.org/10.1007/978-981-15-8677-4

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

This book is gratefully dedicated to all the researchers and editors in the field of Sustainable Communication Networks and Applications.

Foreword

It is with deep satisfaction that I write this Foreword to the proceedings of the ICSCN 2020 held at Surya Engineering College (SEC), Erode, India, during 06–07 August 2020.

This conference brought together researchers, academics and professionals from all over the world, experts in sustainable networking technology, sustainable applications and sustainable computing and communication technologies.

This conference particularly encouraged the interaction of research students and developing academics with the more established academic community in an informal setting to present and to discuss new and current work. The papers contributed the most recent scientific knowledge known in the field of ultra-low-power sustainable system, sustainable vehicular ad hoc networks, Internet-enabled infrastructures for sustainability and sustainable mobility and vehicle management. Their contributions helped in making the conference as outstanding as it has been. The local organizing committee members and volunteers have put much effort ensuring the success of the day-to-day operation of the meeting.

We hope that this program will further stimulate research in sustainable big data frameworks, energy and power-constrained devices, low-power communication technologies, sustainable vehicular ad hoc networks, smart transport systems and smart data analytics techniques.

We thank all authors and participants for their contributions.

Dr. E. Baraneetharan
Conference Chair, ICSCN 2020
Associate Professor & Head
Department of EEE, Surya
Engineering College
Erode, India

Preface

This conference proceedings volume contains the written versions of most of the contributions presented during the conference of ICSCN 2020. The conference provided a setting for discussing recent developments in a wide variety of topics including communications, networks and sustainable applications. The conference has been a good opportunity for participants coming from various destinations to present and discuss topics in their respective research areas.

This conference tends to collect the latest research results and applications on intelligent data communication technologies and networks. It includes a selection of 53 papers from 293 papers submitted to the conference from universities and industries all over the world. All of the accepted papers were subjected to strict peer-reviewing by 2–4 expert referees. The papers have been selected for this volume because of quality and the relevance to the conference.

We would like to express our sincere appreciation to all authors for their contributions to this book. We would like to extend our thanks to the keynote speakers, all the referees for their constructive comments on all papers. Especially, we would

like to thank to the organizing committee for their hard work. Finally, we would like to thank Springer publications for producing this volume.

Dr. P. Karuppusamy
Shree Venkateshwara Hi-Tech Engineering College
Erode, India

Dr. Fuqian Shi
Rutgers Cancer Institute of New Jersey
New Jersey, USA

Dr. Isidoros Perikos
Professor
Department of Computer Engineering
and Informatics
University of Patras
Patras, Greece

Dr. Tu N. Nguyen
Professor
Director of Network Science
Department of Computer Science
Purdue University Fort Wayne
Fort Wayne, USA

Acknowledgements

ICSCN 2020 would like to acknowledge the excellent work of our conference organizing committee, keynote speakers for their presentation during 06–07 August 2020. The organizers also wish to acknowledge publicly the valuable services provided by the reviewers.

On behalf of the editors, organizers, authors and readers of this conference, we wish to thank the keynote speakers and the reviewers for their time, hard work and dedication to this conference. The organizers wish to acknowledge Thiru. Andavar. A. Ramasamy, Ln. K. Kalaiyarasan, Dr. S. Vijayan, Prof. E. Baraneetharan for the discussion, suggestion and cooperation to organize the keynote speakers of this conference. The organizers wish to acknowledge publicly the valuable services provided by the reviewers. Many thanks to all persons who helped and supported this conference. We would like to acknowledge the contribution made to the organization by its many volunteers. We would like to like to acknowledge the contribution made to the organization by its many volunteers and members contribute their time, energy and knowledge at a local, regional and international level.

We also thank all the chairpersons and conference committee members for their support.

Contents

About the Editors

Dr. P. Karuppusamy is working as a Professor and Head in the Department of Electrical and Electronics Engineering at Shree Venkateshwara Hi-Tech Engineering College, Erode, India. In 2017, he had completed doctorate in Anna University, Chennai, and in 2007, he had completed his postgraduate Power Electronics and Drives in Government College of Technology, Coimbatore, India. He has more than 12 years of teaching experience. He has published more than 60 papers in national and international journals and conferences. He has acted as Conference Chair in IEEE and Springer international conferences and Guest Editor in reputed journals. His research area includes modeling of PV arrays and adaptive neuro-fuzzy model for grid connected photovoltaic system with multilevel inverter.

Dr. Isidoros Perikos received the Diploma of Computer Engineer in 2008, the M.Sc. and the Ph.D. on Computer Science from the Department of Computer Engineering and Informatics, University of Patras, in 2010 and 2016, respectively. He is currently an Assistant Professor (adjust) at the Computer Engineering and Informatics Department. His main research interests include artificial intelligence, machine learning, data mining and knowledge extraction, human–computer interaction, natural language processing, and affective computing. He has published over 80 papers in international conferences, journals, and workshops. He is a member of IEEE, ACM, and the Artificial Intelligence in Education Society.

Dr. Fuqian Shi is currently working as a Professor at Wenzhou Medical University, College of Information and Engineering, Prague. He had completed his Ph.D. in Computer Science and Application at Zhejiang University, P.R. China, and completed his M.S. in Control Theory and Engineering at Zhejiang University of Technology, P.R. China. He had published more than 100 papers in national and international journals. He is the reviewer and editorial board member in many reputed journals. His research interest includes computer networks, computer programming, computer graphics, image processing, data structure, operating system, and medical informatics.

Dr. Tu N. Nguyen (Senior Member, IEEE) received the Ph.D. degree in Electronic Engineering from the National Kaohsiung University of Science and Technology (formerly, National Kaohsiung University of Applied Sciences) in 2016. He was a Postdoctoral Associate with the Department of Computer Science & Engineering, University of Minnesota—Twin Cities in 2017. In 2016, he joined the Missouri University of Science and Technology as a Postdoctoral Researcher with the Intelligent Systems Center. He is currently an Assistant Professor with the Department of Computer Science, Purdue University Fort Wayne. His research interests include design and analysis of algorithms, network science, cyber-physical systems, and cybersecurity. He has served as the TPC Chair for the NICS 2019, SoftCOM (25th), and ICCASA 2017, the Publicity Chair for iCAST 2017 and BigDataSecurity 2017, and the Track Chair for ACT 2017. He has also served as a technical program committee member for more than 70 premium conferences in the areas of network and communication such as INFOCOM, Globecom, ICC, and RFID. He has been serving as an Associate Editor for the EURASIP Journal on Wireless Communications and Networking since 2017 and IEEE ACCESS since 2019. He has also been the Editorial Board of Cybersecurity journal, Internet Technology Letters since 2017, the International Journal of Vehicle Information and Communication Systems since 2017, the International Journal of Intelligent Systems Design and Computing since 2017, and IET Wireless Sensor Systems since 2017.

An Emerging Trust-Based Security on Wireless Body Area Network

R. Sudha

Abstract Recent approach in wireless technology leads to WBAN which promises ordinary ambulatory health monitoring for an prolonged period of time and afford real-time advise of the patient's position to the doctor. The drop of privacy is one of the main problem in WBAN. Authentication is the main step against security. Enhanced verification scheme prohibits the networks from pretenders and disturbing users meritoriously. Here proposes a trust-based authentication protocol and its simulation result establishes that they outperform the actual systems in terms of enhanced trade-off among anticipated security holds and computational difficulty.

Keywords Authentication · Security · Onion routing · Digital signature · WBAN

1 Introduction

Security in any wireless technology especially in wireless body area networks is highly needed. Authentication process is solitary of the preliminary steps for security employed to put off from the unconstitutional users and pretenders. Authentication schemes vary as per the nature of wireless body area network. For such networks, there is a need of specific lightweight authentication schemes. Security begins with a transaction of wanted security suite between the two conveying the gatherings, hub, and center point. The security choice sets off a security relationship between the two gatherings. To actuate a pre-shared or creating another mutual ace key. Security affiliation conventions are done in view of the key trade arrangements.

The process region of a WSN is extremely huge and can be used in ecological observing, manage temperature and moisture, vehicle transfer control, checking of human body organs, and among others. Figure 1 exemplifies a situation of WBANs in the medical area where patients that are being observed can be in a hospital, at

R. Sudha (✉)
Associate Professor & Head, Department of Computer Science, PSG College of Arts & Science, Coimbatore, India
e-mail: sudha279@yahoo.com

P. Karuppusamy et al. (eds.), *Sustainable Communication Networks and Application*, Lecture Notes on Data Engineering and Communications Technologies 55,
https://doi.org/10.1007/978-981-15-8677-4_18

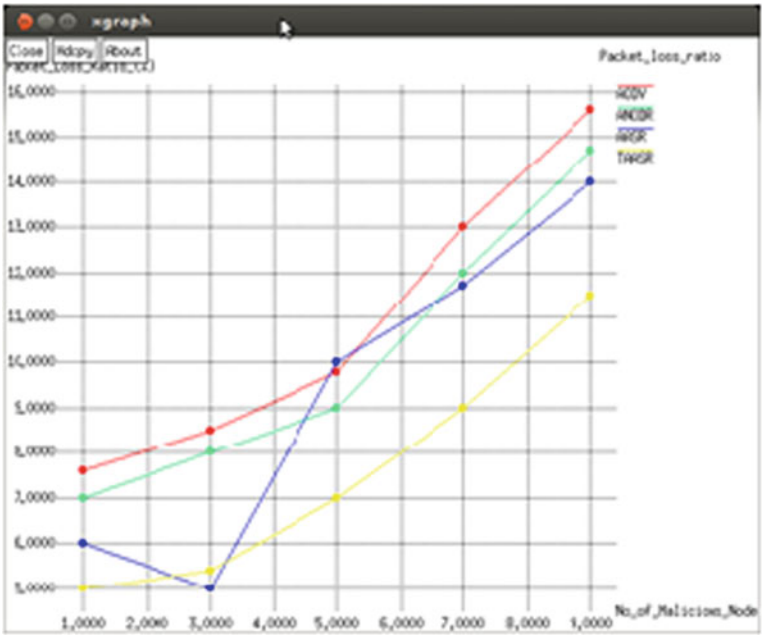

Fig. 1 Comparison based on packet loss ratio

home, or anyplace besides performing an goings-on routine. Sensing data are send to health experts in the course of the Internet.

The fundamental security requirements in WBAN are described below [1].

1. Data Confidentiality. To protect the data from a revelation, the system necessitates data discretion
2. Data Authentication. Applications together with mutually medical and non-medical relevance demand data authentication. Symmetric technique can be used in a WBAN to attain data authentication. This method shares the secret key to work out Message Authentication Code for all data.
3. Data Integrity. This is compulsory as an rival can modify the data that is broadcasted over an anxious channel. Deficiency of data integrity system paves a way to the opponent to amend the information before it reaches the destiny.

2 Related Work

In order to obtain the issues in existing wireless body area networks, a vast survey has been made based on wearable gadgets and wireless body area networks. Sensors play a vital role in body area networks. In few research models mentioned that sensors must be constructed based on cryptographic parameters since it is major challenge in WBAN to meet necessary security measures [2, 3]. In few research

models, biometrics is considered as an important factor since it describes the relation of the individual in an unique manner and helps to secure the system communication between wireless body area networks [4]. Various security mechanisms are evolved in wireless body area networks based on symmetric cryptosystem. The system restricts the access to the assets if it faces any issues. However, it lags to provide security against physical arrangements in some cases [5].

Other than the intricacy of detecting component, hub's key administrations in WBAN offer each part abundance. On the different, some exploration misuses the awry cryptosystem in portable and specially appointed systems even have been expected, and attempted to appear at the peculiar uniqueness of WBAN [6, 7]. One misery about the topsy-turvy cryptosystem is a source imperative inconvenience; however, current work has demonstrated that performing ECC devours a considerable measure a lesser measure of memory and processing power [7]. These investigates tended to a span of controlled body area networks and avoid the discussion about sensor systems implantation. Wireless body area networks work based on the arranges of connected elements in human body and the communication is possible from any place. Recent framework discussed in [8, 9] provides communication process in inter- and intra-wireless body area networks in telemedicine application. Using wireless module like Bluetooth for short-range and ZigBee for long-range communication, the proposed model dispatches the data from sensors to the sink. Sathesh [1, 10] discussed the importance of rack remote sensors and developed the wireless body area network model similar to Tmote sky design.

An end-to-end mhealth application for patient monitoring is discussed [11] as European MobiHealth venture which progress based on GPRS and UMTS. Using assorted sensors, the vital signs such as electrocardiogram, circulatory strain, pulse are continuously monitored in mobihealth setup. Communication through the sensors is performed thorough exceptional gadget which works based on single-hop ZigBee or Bluetooth module. The fundamental issues in health applications are considered in terms of insurance, dependability of correspondence assets, and quality of service ensures. The French undertaking BANET [12] means to develop a structure, copies, and instruments to mode improved remote correspondence frameworks proposing the greatest differentiation of WBAN-based applications, contained by the customer regular reasoning, restorative, and game fields. The investigation reports the issues in expansion channels in WBAN and its MAC conventions along with substitute remote systems. Falck et al. [13] discussed about the German BASUMA venture and its wireless body area networks based on the framework. The design has UWB in its front end along with IEEE 802.15.3 as MAC decorum. This system also utilizes time allocations based on opening schedules by getting the period disputes through CSMA/CA communication process.

In literature [14], an economic bendable wireless body area network for urbanized utilization. The objective of the research present in terms of developing location-based application which helps to obtain results in the on field testing. Sensors such as WiMoCA-hubs are used in the experimental process and the sensors could be placed anywhere since it is characterized by MEMS accelerometers, and the performance will not be deviated. The exploration of wearable sensors is focused in IBBT IM3

[15] which helps to analyze the wearables of the patients. In this process, a heat beat is used to detect and send to medical specialists and provide solution to the patient. Based on cryptosystems, the security of the wireless body is network and is analyzed in literature [16]. Cryptosystems are used to validate the risks in WBAN and provide strong security to the system. From the survey, it is observed that almost all the models have limitations in its security factors. Very few models are analyzed the issues related to security in mobihealth applications. Based on the observed limitations, the proposed models are formulated in the following section.

2.1 Trust and Security Issues

Data security is for the most part in view of two elements: trust and security. In WBAN, every hub is engaged with the bundle exchange ought to guarantee that their neighboring hubs are trustful and secure. The component which verify that the data about the source is really who it professes to be. The signatures and encryption instruments should require an arrangement to check by any hubs the wellsprings of that data. Security and trust are firmly commonly subordinate element that cannot be distanced.

2.2 Proposed Methodology

We indicate a WBAN by B and make the accompanying suspicions.

2.2.1 Group Signature

Gathering signature is a strategy for enabling individuals from a gathering to sign namelessly in a WBAN steering convention. Gathering signatures can be seen as customary open key marks with extra protection highlights. This approach is to run a gathering key assention convention toward the start of each schedule vacancy and utilize the subsequent gathering key as the normal parameter and versatile. The more productive approach is to utilize a gathering key understanding convention with a specific end goal to concede to the normal parameter and gathering chief to create and convey this beginning worth. Gathering signature conspire has bunch administrator, who is reaction for including new individuals and denying mark of individual hubs in obscurity are given to a gathering supervisor.

Open Key GB+: key this is normal to every one of the hubs of a gathering B.

Private Key GN1−: key which gives security for the information of individual hub N1 in a gathering B where N1 $\in$ B.

Hub N1 uses GN1 private key to sign a message, and this signed message can be unscrambled by means of people in general key GB+ by alternate hubs in B, which keeps the obscurity of N1 [17].

2.2.2 Onion Routing

The fundamental work of onion steering convention is foundation of association and taking into consideration unidentified correspondence. Amid Route ask for the messages are dully encoded the data while sent source to goal hubs of onion switches [18]. While in Route-Request has each transitional hubs known as onion switches seizes a layer of encryption and uncover directing data when pushes the message from goal to the source hub. This system safeguards these go-between hubs about knowing the cause, goal, and substance of the message. To pass an instant message, the directing onion is an information structure which frames concealed layer by encryption for sending an instant message with back-to-back layers of encryption. In the meantime while back warding an instant message, it unscrambles their relating layer and the first plaintext message visible just to sender and beneficiary. It is end-to-end encryption and decoding process between the source and the goal in ill-disposed condition.

3 Proposed Work

Many trust administration plans have been proposed to assess trust esteems and the vast majority of the trust-based conventions for secure directing computed trust esteems in light of the qualities of hubs carrying on appropriately at the system layer. Trust estimation can be application subordinate and will be diverse in light of the outline objectives of proposed plans. The trust administration measurements incorporate overhead (e.g., control parcel overheads), throughput, bundle conveyance proportion, bundle dropping rate, and postponement.

3.1 Public Key Cryptography

For onion directing, the messages are scrambled and unscrambled utilizing PKC. In this paper, we have utilized elliptic curve Diffie Hellman key trade calculation.

3.2 Public Key Encryption

The secrecy of correspondence is achieved by public key encryption (PKE) amid transmission.

Here, the sender utilizes the general population key of the beneficiary to scramble the substance of the message. The enciphered message is then transmitted to the recipient and the collector would then be able to utilize their own coordinating private key to decode the message.

3.3 Elliptic Curve Diffie Hellman Key Exchange Algorithm

ECDH is utilized for the motivations behind key understanding. Assume two hubs, n1 and n2, wish to trade a mystery key with each other. N1 will create a private key dA and an open key QA = dAG (where G is the generator for the bend). Essentially, n2 has his private key dB and an open key QB = dBG. In the event that n2 sends its open key to n1 then ready to figure dAQB = dAdBG. Also if n1 sends its open key to n2, at that point he can compute dbQA = dAdBG. The mutual key is the x co-ordinate of the computed point dAdBG. Any busybody would just know QA and QB, and cannot ready to appraise the common mystery key.

3.4 Digital Signature

The objective of an advanced mark conspire is to guarantee the sender of the message cannot disavow a message that they sent. Accordingly, the motivation behind computerized marks is to guarantee the non-denial of the message being sent. This is helpful in a down to earth setting where a sender wishes to make an electronic buy of offers and the recipient needs to have the capacity to demonstrate who asked for the buy.

3.5 Protocol Design

The personality data is appointed to every hub in instatement stage or when the hub will be designed.

3.6 Trusted Anonymous Route-Request

In the proposed conspire, initially, every hub will be arranged with the steady trust esteem 50 utilizing hub trust work. The proposed convention can choose the better way (trusted and briefest) utilizing trust esteem and the quantity of bounces. At the point when the RREQ and RREP message are created in the system, every hub add its own trust an incentive to the trust aggregator on these course revelation stage. Every hub likewise refreshes its own particular steering table. The accompanying recipe can be utilized to assess the trusted and briefest way.

Entirety of trust esteems Where, Sum of trust esteem $= \sum$ trustvalue (I).

3.7 Trusted Routing Procedure

The directing calculation can be actualized in view of the current on-request impromptu steering convention like AODV. The primary directing methods can be condensed as takes after:

1. During course disclosure, two stages are performed
   (a) First before sending the RREQ, the trust estimation of each neighboring hub is introduced to 50
   (b) Second source hub communicates a RREQ parcel in the arrangement to find confided in neighbors.
2. If a transitional hub gets the RREQ bundle, it checks the RREQ by utilizing its gathering open key, and includes one layer best of the key-scrambled onion. It checks the trust estimation of the neighbor hub and in light of the trust factor, the hub chooses its next neighboring hub for RREQ bundle exchange. This procedure is rehashed until the point when the RREQ parcel achieves the goal or terminated.
3. Once the RREQ is gotten and checked by the goal hub, the goal hub collects a RREP bundle in the arrangement and initiates communication with source hub.
4. On the invert way back to the source, each moderate hub approves the RREP bundle and updates its directing and sending tables.
5. Then it expels one layer on the highest point of the key-encoded onion, and keeps broadcasting the refreshed RREP in the arrangement.
6. When the source hub gets the RREP parcel, it verifies the bundle, and updates its steering and forwarding tables. The course revelation stage is finished.
7. The source hub begins information transmissions in the set up course in the arrangement. Each intermediate node advances the information bundles by utilizing the route pseudonym.

4 Experimental Result

The Random Way Point Mobility Model portrays the development of hubs. The respite time is set to 10 s. what's more, most extreme speed set to 5 m/s. The recreation time is set to 100 s. furthermore, nodes are similarly dispersed in 800 × 800 m zone. Subsequent to getting the estimations of every execution metric as indicated by every convention, the diagram has been plotted to demonstrate the examination between AODV, ANDOR, AASR and TAASR.

As appeared in Fig. 1, the proposed TAASR has most astounding capacity to distinguish packet dropping ratio with the assistance of its trust administration approach and it beats the current strategies AODV, ANDOR and AASR. AASR accomplishes 5% more prominent misfortune proportion than TAASR in normal.

As appeared in Fig. 2, while there is increment in number of malevolent hubs, the normal throughput of four protocols diminishes clearly. Throughput of the proposed TAASR is higher than the staying existing protocols.

Figure 3 depicts the analysis of end-to-end delays. In this TAASR invest energy in the security handling in their course revelation, its postponement is higher than AODV. On the off chance that ANODR is under a substantial assault, it will dispatch new course disclosures for the broken courses, which present more deferrals in normal. Contrasted with the assaulted ANODR, AASR, and AODV, the proposed TAASR decreases the need of re-steering because of its trust-based validation and onion directing which results in 20 ms less of deferral in normal.

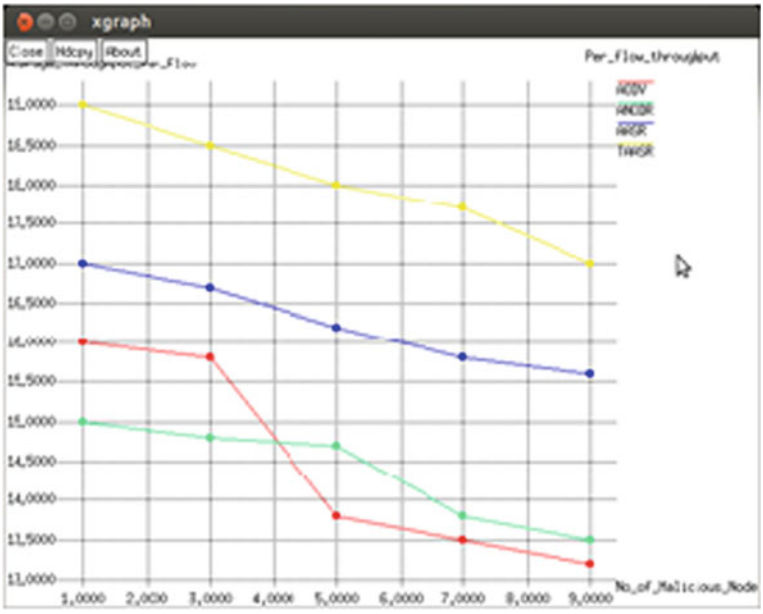

Fig. 2 Comparison in light of throughput

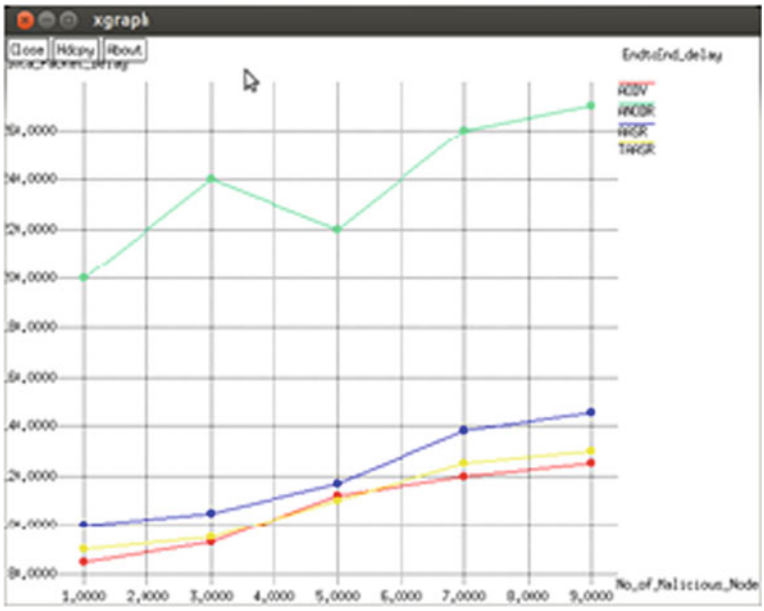

Fig. 3 Comparison in light of end-to-end delay

Performance Evaluation of Mobile Scenario Under Adversarial Environment:

To mimic the adversarial conditions, the aggregate nodes are set into 20% of its actual value, i.e., 9 nodes, as malignant nodes. The system portability is changed from 1 to 5 ms and record the execution consequences of the four protocols (Fig. 4).

In spite of the execution variety, TAASR dependably accomplishes the most elevated throughput because of its trust-based taking care of nature. This can be clarified by its capacity in protecting the bundle dropping assault.

The bends of the end to-end delay are appeared in Fig. 5. Because of the extra security preparing time in RREQ flooding, AODV, ANODR, and AASR have longer postponements than TAASR, while AASR has 20 ms less of deferral than TAASR in normal (Fig. 6).

5 Conclusion

The trust and trust relationship among nodes can be spoken to, figured and consolidated utilizing a thing feeling. In our TAASR proposed protocol, nodes can participate together to get a target sentiment about another node's reliability. They can likewise perform confided in directing practices based on the trust relationship. With a conclusion limit, nodes can adaptably select the method to execute cryptographic process. Consequently, the computational overheads are lessened without the need of asking

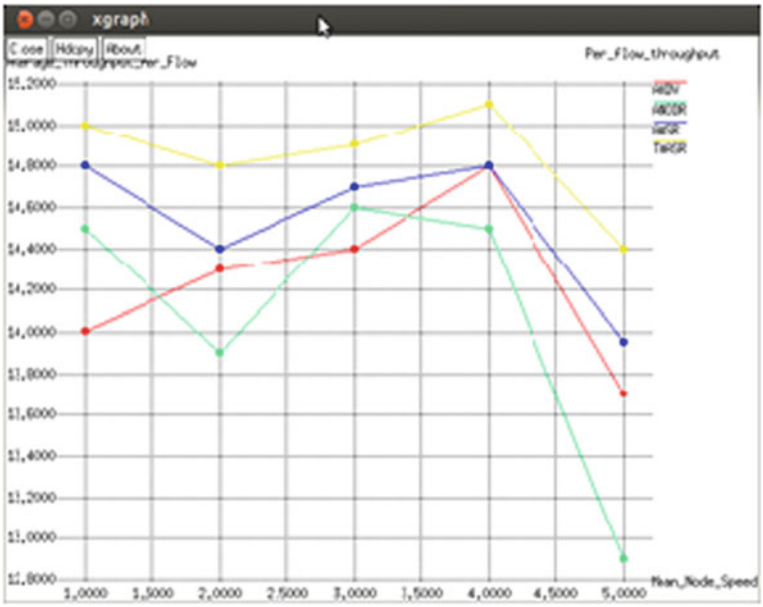

Fig. 4 Performance correlation in light of throughput

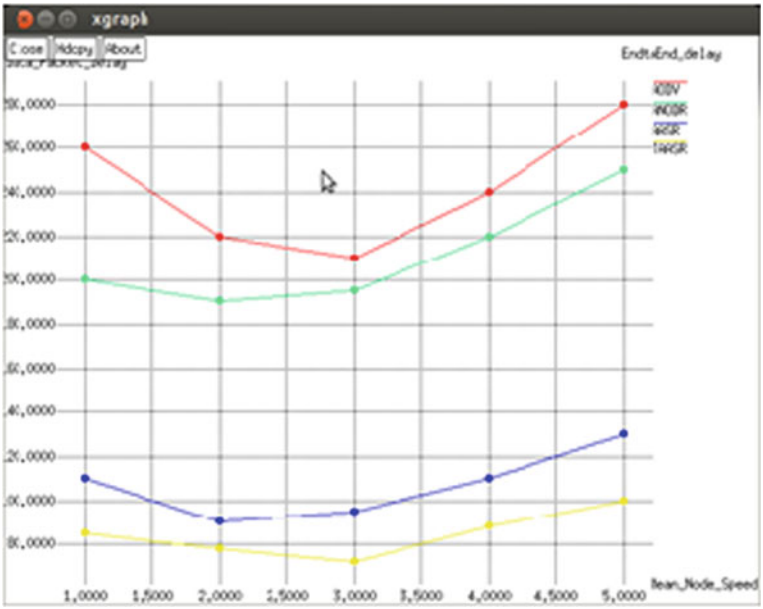

Fig. 5 Performance correlation in light of end-to-end delay

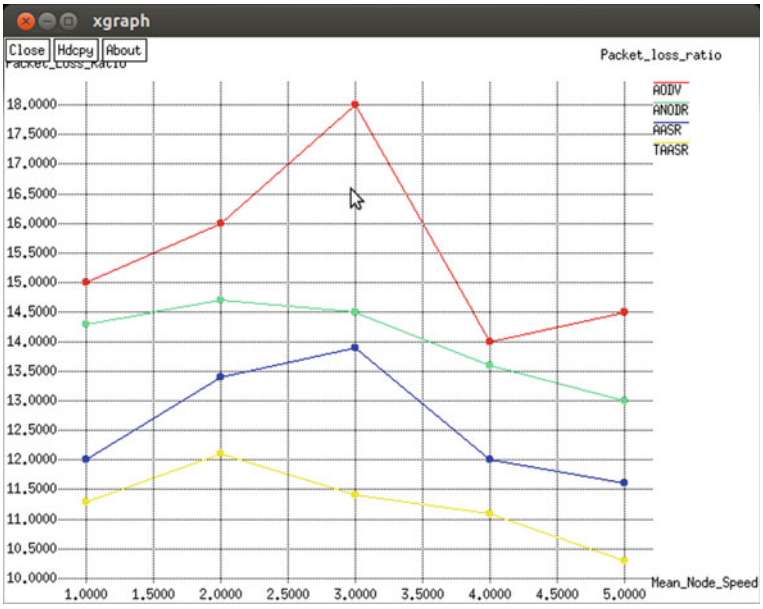

Fig. 6 Performance correlation in light of packet loss ratio

for and checking declarations at each directing activity. Our TAASR steering convention is an all the more lightweighted; however, more adaptable security arrangement than other cryptography and confirmation plan. It utilizes trust esteems to support parcel sending by keeping up a trust counter for every node. On the off chance that the trust counter esteem falls underneath a limit, the comparing halfway hub is noxious node. In this proposed conspire, approved node has high throughput and parcel conveyance proportion can be enhanced altogether with diminishing normal end-to-end delay by expanding trust esteem.

References

1. Sathesh, A.: Optimized multi-objective routing for wireless communication with load balancing. J. Trends Comput. Sci. Smart Technol. (TCSST) **1**(02), 106–120 (2019)
2. Poon, C.C.Y., Zhang, Y.T., Bao, S.-D.: A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. Commun. Mag. IEEE **44**, 73–81 (2006). https://doi.org/10.1109/MCOM.2006.1632652
3. Sudha, R., Devapriya, M.: A survey on wireless body sensor networks for health care monitoring. In: Int. J. Sci. Res. (IJSR) **3**(9), 1574–1578 (2014)
4. Sudha, R., Devapriya, M.: Enhanced bio-trusted anonymous authentication routing technique of wireless body area network. In: Biomedical research 2016 in Special Issue: S276–S282, September 2016
5. William, C., Tan, C.C., Wang, H.: Body sensor network security: an identity-based cryptography approach. In: Proceedings of the ACM conference on wireless network security (WiSec '08),

pp. 148–153. ACM Press (2008). https://doi.org/10.1145/1352533.1352557
6. Lim, S., Oh, T.H., Choi, Y.B., Lakshman, T.: Security issues on wireless body area network for remote healthcare monitoring. IEEE Int. Conf. Sens. Netw. Ubiquitous Trustworthy Comput. **2010**, 327–332 (2010). https://doi.org/10.1109/STUC.2010.61
7. Sharmilee, K.M., Mukesh, R., Damodaram, A., Subbiah Bharathi, V.: Secure WBAN using rule-based IDS with biometrics and MAC authentication. In: 2008 10th IEEE international conference on ehealth networking applications and services, pp. 102–107. IEEE (2008). https://doi.org/10.1109/HEALTH.2008.4600119
8. Otto, C., Milenkovic, A., Sanders, C., Jovanov, E.: System architecture of a wireless body area sensor network for ubiquitous health monitoring. J. Mobile Multimedia **1**(4), 307–326 (2006)
9. Jovanov, E., Milenkovic, A., Otto, C., de Groen, P.C.: A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. J. NeuroEng. Rehab. **2**(1), 16–23 (2005)
10. Moteiv [online] https://www.moteiv.com
11. van Halteren, A.T., Bults, R.G.A., Wac, K.E., Konstantas, D., Widya, I.A., Dokovski, N.T., Koprinkov, G.T., Jones, V.M., Herzog, R.: Mobile patient monitoring: the mobihealth system. J. Inf. Technol. Healthcare **2**(5), 365–373 (2004)
12. Bhalaji, N.: QOS and defense enhancement using block chain for fly wireless networks. J. Trends Comput. Sci. Smart Technol. (TCSST) **1**(01), 1–13 (2019)
13. Falck, T., Espina, J., Ebert, J.P., Dietterle, D.: BASUMA—the sixth sense for chronically ill patients. In: International workshop on wearable and implantable body sensor networks (BSN), pp. 57–60, Cambridge, MA, USA, 3–5 April 2006
14. Farella, E., Pieracci, A., Benini, L., Rocchi, L., Acquaviva, A.: Interfacing human and computer with wireless body area sensor networks: the Wimoca solution. Multimedia Tools Appl. **38**(3), 337–363 (2008)
15. Pandian, M.D. :Enhanced network selection and handover schema for heterogeneous wireless networks. J. ISMAC **1**(01), 160–171 (2019)
16. Jang, C.S., Lee, D.G., Han, J.W., Park, J.H.: Hybrid security protocol for wireless body area networks. Wirel. Commun. Mobile Comput. **11**, 277–288 (2011). https://doi.org/10.1002/wcm.884
17. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Proceedings of CRYPTO, pp. 41–55 (2004)
18. Zhang, Y., Liu, W., Lou, W., Fang, Y.: MASK: anonymous on-demand routing in mobile ad hoc networks. IEEE J. Wirel. Commun. **5**(9), 2376–2385 (2006)