Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol.7, No.3, September 2019, pp.1126-1137
Available online at: http://pen.ius.edu.ba

Lightweight novel trust based framework for IoT enabled wireless network communications

Somnath B. Thigale[1], Rahul K. Pandey[2], Prakash R Gadekar[3], Virendrakumar A. Dhotre[4], Aparna A Junnarkar[5]

[1]Ph.D Research Student MUIT
[2]Ph.D Guide MUIT
[3]Ph.D Research Students MUIT
[4]Ph.D Research Students MUIT
[5] Professors, PES Modern College

Article Info

Received Jun 12th, 2019

Keyword:

Internet of things
data communication
security
privacy
cryptography
trust management

ABSTRACT

For IoT enabled networks, the security and privacy is one of the important research challenge due to open nature of wireless communications, especially for the networks like Vehicular Ad hoc Networks (VANETs). The characteristics like heterogeneity, constrained resources, scalability requirements, uncontrolled environment etc. makes the problems of security and privacy even more challenging. Additionally, the high degree of availability needs of IoT networks may compromise the integrity and confidentially of communication data. The security threats mainly performed during the operations of data routing, hence designing the secure routing protocol main research challenge for IoT networks. In this paper, to design the lightweight security algorithm the use of Named Data Networking (NDN) which provides the benefits applicable for IoT applications like built-in data provenance assurance, stateful forwarding etc. Therefore the novel security framework NDN based Cross-layer Attack Resistant Protocol (NCARP) proposed in this paper. In NCARP, we designed the cross-layer security technique to identify the malicious attackers in network to overcome the problems like routing overhead of cryptography and trust based techniques. The parameters from the physical layer, Median Access Control (MAC) layer, and routing/network layer used to compute and averages the trust score of each highly mobility nodes while detecting the attackers and establishing the communication links. The simulation results of NCARP is measured and compared in terms of precision, recall, throughput, packets dropped, and overhead rate with state-of-art solutions.

1. Introduction

Despite different researches on Intent of Things (IoT), its definition remains fuzzy. The IoT is the collection of physical devices that are connected to the Internet. With the advancement in mobile computing and wireless communications, a new paradigm known as the Internet of Things (IoT) is swiftly generating a lot of research interest and industrial revolution [1]. Users will feel insecure about their private data if they are vulnerable to attacks from unauthorized individuals or machines over the network. Thus security is by far one of the biggest challenges in IoT networks [3]. Most of security threats are performing at the routing layer, it means during the data transmission process, thus the addressing strong security against such threats will be depends on the security mechanism designed in routing functionality. However, the cross-layer attacks also increasing now-a-days to disturb the communication networks at large extend. Thus, making the process of secure communications in IoT is even more challenging. This imperative need for securing the routing process between numerous IoT devices across multiple heterogeneous networks needs significant research contributions [4] [5]. To mitigate the challenges of secure routing in IoT enabled networks, there are various solutions designed at routing layer since from last decade. The security solutions designed to detect and mitigate the security threat such as botnets, Denial-of-Service (DoS), malware, Distributed Denial-of-Service (DDoS), Man-In-Middel (MIM) attacks, jamming attacks etc.

In this paper, we focused on. The smart cities consist of large number of IoT physical devices deployed in a range of settings from individual homes to critical infrastructure, potentially in a very dense deployment. The intelligent traffic monitoring is one of the most important and challenging part of IoT based smart cities in which the vehicles with high mobility needs to monitor effectively. The Vehicular Ad hoc Networks (VANETs) consist of large number of vehicles in city roads which needs the strong guarantees of security as the sensitive information circulated by the vehicles to monitor the conditions like traffic jam, accidents etc. Thus it is required to have end-to-end security and privacy mechanism in the networks like IoT enabled VANET.

In this paper, our aim is to design robust solution which is takes the advantages of NDN mechanism and cross-layer technique to secure the IoT enabled wireless network communications [6]. As observed in recent woks, the Information Centric Networking (ICN) technology is superior to Internet Protocol (IP) technology while working with the IoT networks [7]. The NDN is significantly stronger for the efficient and scalable smart city applications using the features like in-network caching and stateful forwarding [8]. In literature, various ICN based IoT instalments proposed, but there is no holistic NDN based IoT architecture yet proposed [9]-[11]. Basically, the current works neglects the security concerns related to the on-boarding and secure routing. In this paper, we exploit the benefits of NDN architecture over the IP architecture while performing the routing in IoT enabled VANETs. The NDN based secure cross-layer trust based communication protocol designed called NCARP. The proposed NCARP protocol is trust based approach in which the trust of vehicular nodes computed using different layers parameters such as physical, MAC, and routing layer to detect the node as malicious or attacker. In section II, the brief review various security methods presented. In section III, the proposed model of NCARP technique with parameters used for the trust computation presented. In section IV, the simulation and evaluations of NCARP with recent methods presented. In section V, the conclusion and future direction based on the simulation outcomes disclosed.

2. Related Works

This section we present the review of different security solutions for wireless communications. As the proposed framework is based on cross-layer and trust based approach, we majorly reviewed such methods. In networks like VANET, the aim of trust based approaches to assess the behaviours of the wireless nodes and build the reputation of every node according to their behaviour scores. In [12]-[21], various trust based security methods presented for VANET communications.

The proposed work in this paper is different and based on NDN architecture where we utilized the three layers parameters to evaluate the trust of high mobility nodes. To the best of our knowledge this is first approach that covers the cross-layer architecture for IoT enabled VANETs as well as NDN architecture to achieve the more reliable and robust communications with minimum routing overhead. The NDN approach recently designed in [32]. In [32], the recent NDN based security approach proposed IoT networks. Scalability is achieved through a hierarchical network design, and very little cryptographic or computational burden. However the work at just initial stage and failed to handle the problem of nodes mobility and overhead reduction.

3. Methodology

As described above, the NCARP protocol proposed in this paper to achieve the reliable and secure communications in IoT enabled VANETs with minimum overhead. We mainly focused on using the ICN based NDN architecture over the IP. To establish the reliable links, the cross-layer trust score computed to evaluate the trustworthiness of vehicles. In this section we first take the overview of NDN approach used in NCARP, and then present the cross-layer framework for network security and reliability.

A. NDN Framework

The "slight abdomen" of the Named Data Networking (NDN) stack, as the name infers, is Named Data. In the NDN model, each piece of information has a novel Name, like a Uniform Resource Identifier (URI); the substance related with each Name is ordinarily viewed as unchanging. To recover a specific substance object, a requester sends an Interest parcel into the system.

Router: Every switch in NDN keeps up three information structures: a Pending Interest Table (PIT), a Forwarding Information Base (FIB), and a Content Store (CS). The sending methodology for the two Interests and Data are based around these tables.
The switch at that point includes another PIT section demonstrates that the Interest was sent.

Data Forwarding: Information parcels are basically sent after the invert way as demonstrated by coordinating PIT passages. Note that the configurability of the sending technique is a significant element for the utilization of NDN in IoT. We utilized the NDN based correspondence engineering and expect that the supporting layers, for example, MAC, Physical, information connection layers depend on NDN design in this work.

B. Cross-Layer Architecture

Figure 1 demonstrates the architecture of proposed NCARP protocol.

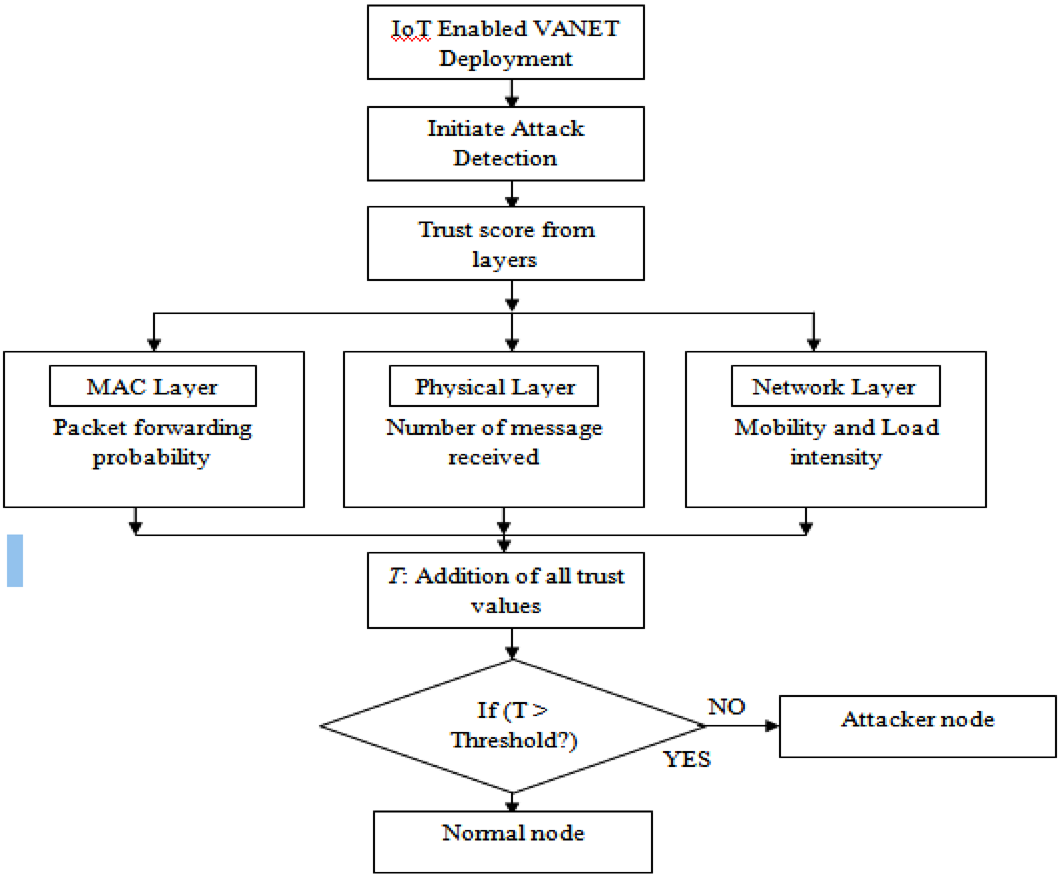
IoT Enabled VANET Deployment
Initiate Attack Detection
Trust score from layers
MAC Layer
Packet forwarding probability
Physical Layer
Number of message received
Network Layer
Mobility and Load intensity
T: Addition of all trust values
If (T > Threshold?)
NO
YES
Attacker node
Normal node

Figure 1. NCARP protocol architecture

The NCARP protocol is designed to efficiently detect the malicious node in network according to the trust values from physical layer, MAC layer, and network layer. The IoT enabled VANET network deployed with *N* number of vehicles in network. After the deployment we initiated the trust computation for each node in network at different layers. At physical layer we compute the number of message received from the Vehicle Node (VN). At the MAC layer, we mainly focused on VN Packet Forwarding Probability (PFP) which is based on number of re-transmission factor as well. Finally, the network layer, to select the *VN* as forwarder node, we must compute its current mobility speed and the load intensity value. Finally, the overall trust value of any *VN* is computed as the addition of all layers trust value of *VN* at time *t*. After computation of overall trust value of VN, that value is compared with pre-defined threshold value to detect and inform the malicious node in network. The parameters used to compute at each layer are elaborated below.

A. MAC Layer Trust: In networks like VANET, due to the higher mobility, there are several other reasons behind the packet drops in network. While transmitting packets though the hops, if next hop is goes out of range due to mobility then it leads to packet loss. The MAC layer information is one of the most important parameters in order to analyze the possible causes for packet loss between two nodes. In this paper, to compute the MAC layer trust we measure the PFP between two nodes P and Q. In this case, the node P measures the probability of successfully packet transmission to node Q by observing the link layer quality between P and Q using HELLO messages. This MAC layer trust value is represented as T_k^{MAC} for the k^{th} VN. The PFD at MAC layer between two VNs computed as at time *t*:

$$T_k^{MAC}\,(t) = \frac{\sigma_{recv}\,(t_{i-1},t_i)}{\sigma_{exp}(t_{i-1},t_i)} \qquad (1)$$

Where σ_{recv} and σ_{exp} total number of HELLO packets received and expected number of HELLO packets during the time interval(t_{i-1},t_i). Higher the value of T_k^{MAC}, better the chances of node *k* marked as legitimate node.

B. Network Layer: At network layer, routing is major task to deal with malicious attackers and to prevent the packet losses. In highly dynamic networks, the node with sever mobility and traffic load is consider as the malicious or unreliable node for the data forwarding. Thus, to compute the trust at network layer we computed the load intensity and mobility speed of the VN.

Load Intensity: In IoT enabled VANETs, queues may overflow due to the multiple simultaneous roles that nodes have, such as being routers and terminals as well as multi-hop forwarding nodes, and to the frequent transmission of topology messages.. We compute the load intensity based trust value for each VN in network.

$$(LI)^k = \frac{\mathrm{A}^{\mathrm{k}}}{q_{max}^k} \qquad (2)$$

Where q_{max}^k is the length of interference queue of node *k*.The $A^k$is average traffic load at the node *k* at time *t*. Using the above value, we finally compute the trust score of load intensity parameter for node *k* as:

$$T_k^{Load} = 1-(LI)^k \qquad (3)$$

Node Mobility: Another very important parameter to select the more stable and reliable VN as forwarder in V2V communications. We measure the current moving speed of the vehicle in this paper and compute its probability value.

$$(LCR)^{\mathrm{k}} = \frac{\sigma^{\mathrm{k}}+\gamma^{\mathrm{k}}}{\max(\sigma^{\mathrm{k}})+\max\,(\gamma^{\mathrm{k}})} \qquad (4)$$

Where, σ^{k} is the link arrival rate and γ^{k} is the link breakage rate of node *k*. By using the Eq. (4), the mobility based trust score is computed as:

$$T_k^{Mobility} = 1-\ \mathrm{LCR}^k \qquad (5)$$

By considering both load intensity and node mobility, the network layer trust score for each VN computed T_k^{NET} for the k^{th}*VN* as at time *t*:

$$T_k^{NET}(t) =\ T_k^{Load} +\ T_k^{Mobility} \qquad (6)$$

Higher the value of T_k^{NET}, better the chances of node *k* marked as legitimate node.

C. Physical Layer Trust: In networks like IoT enabled VANET, the common security problem is jamming the network attack in which the attacker or malicious vehicle frequently transmits the short range signals which creates the network congestion. Due to this network congestion, the normal vehicle remains busy in receiving such signals and rejects the other application needs. Therefore, Number of Received Messages (NRM) is used to evaluate the trustworthiness of vehicles in network at physical layer. The monitoring VN collects the observations of NRM from its neighbor VNs at every time period *t*. The recommendations of NRM values generated by the direct observations of neighbor nodes *n* with the monitored k^{th}*VN*. The trust value based on above computations at physical layer for the k^{th}*VN* is computed as:

$$T_k^{PHY}(t) = (NRM^k - \frac{1}{n}\sum_{i=1}^{n} NRM^n) \ / \ \frac{1}{n}\sum_{i=1}^{n} NRM^n \qquad (7)$$

Higher the value of T_k^{PHY}, better the chances of node k marked as legitimate node.

Thus, the overall trust of k^{th}*VN* at time *t* is computed as:

$$T_k(t) = \alpha 1 \times T_k^{PHY}(t) + \alpha 2 \times T_k^{MAC}(t) + \alpha 3 \times T_k^{NET}(t) \qquad (8)$$

Where $\alpha 1$, $\alpha 2$, and $\alpha 3$ are weight parameters and whose sum ($\alpha 1 + \alpha 2 + \alpha 3 = 1$). The value of these weight parameters should in range of (0, 1). F

Algorithm 1: Trust based attack detection

Inputs
N: number of vehicles
S: source node
δ=0.45: threshold value
***Output*:**
V: detected attackers node list

```
FOR k= 1: N
    Compute MAC layer trust score: $T_k^{MAC}$ using Eq. (1)
    Compute network layer trust score: $T_k^{NET}$using Eq. (6)
    Compute physical layer trust score: $T_k^{PHY}$using Eq. (7)
    Averaging the trust value: $T_k$using Eq. (8)
        IF ($T_k > \delta$)
    k ='normal'
    ELSE
    k ='malicious'
            V = {V; k}
    END IF
    END FOR
```

4. Simulation Results

In this section, our objective is to design the proposed NCARP protocol and two recent methods those are based on trust based concept and Cryptography base concept for secure VANET communications. The methods such as RealAlert [18] which is trust based security method for vehicular networks and cryptography based method reported in [17], we called this method as MANEL (the name of author). Table 1 demonstrate the other simulation parameters used. Table 2 demonstrate the another network scenario where we kept number of vehicle fixed and vary the percentage of malicious nodes in network.

Table 1. IoT enabled VANET design parameters (density variations)

Number of vehicles	50, 100, 200
Simulation Time	500 second
Mobility (Km/s)	40 km/h
Secure methods	RealAlert, MANEL, and NCARP
MAC	IEEE 802.11p
Propagation Model	Two-Ray Ground
Mobility	Random Walk Mobility
Antenna	Omni Antenna
CBR Connections	5-10
Network size	7000 x 7000
Number of Malicious Nodes	10 %

Table 2. IoT enabled VANET design parameters (Attackers variations)

Number of vehicles	100
Simulation Time	500 second
Mobility (Km/s)	40 km/h
Secure methods	RealAlert, MANEL, and NCARP
MAC	IEEE 802.11p
Propagation Model	Two-Ray Ground
Mobility	Random Walk Mobility
Antenna	Omni Antenna
CBR Connections	5-10
Network size	7000 x 7000
Number of Malicious Nodes	5 % to 40 %

The performance of these methods measured in terms of precision rate, recall rate, average throughput, number of packets dropped, and communication overhead. The precision and recall rates estimate the accuracy of malicious nodes detection. The average throughput, number of packets dropped, and communication overhead demonstrates the QoS performance.

A. Density Variations

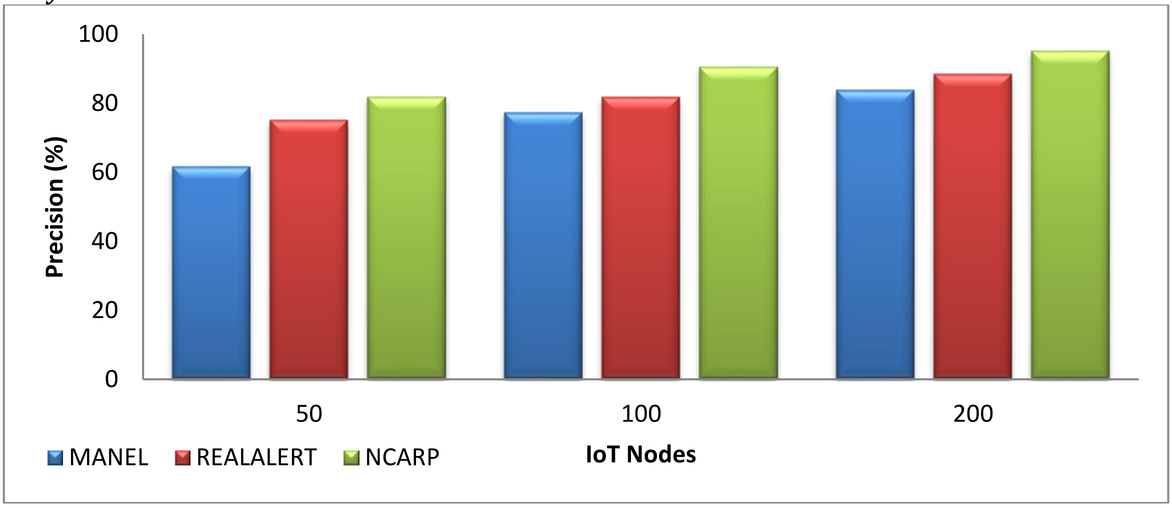

Figure 2. Performance analysis of precision rate

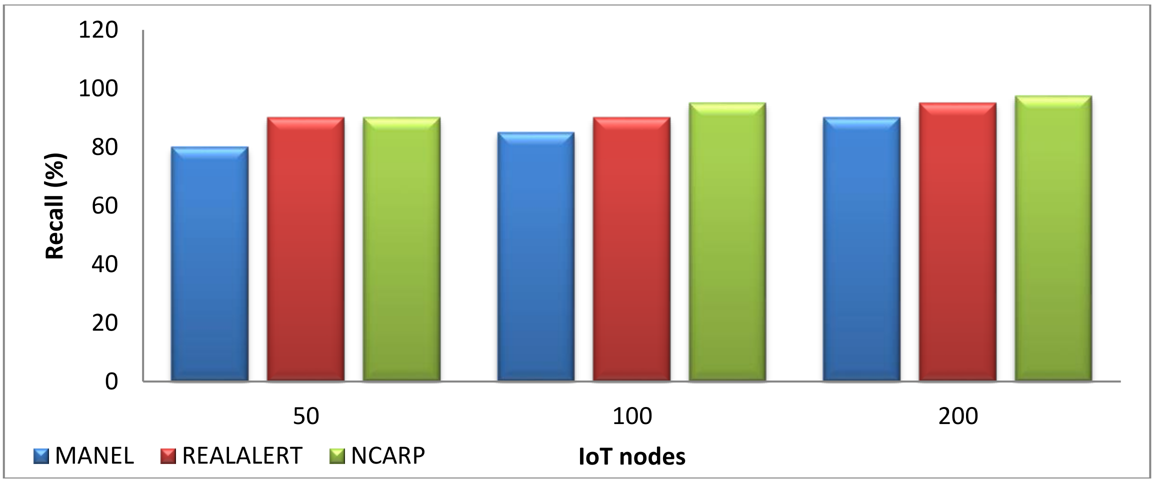

Figure 3. Performance analysis of recall rate

Figure 2 and 3 demonstrate the attacks detection accuracy using all the three methods. The performance of NCARP proves the efficiency in successful attacks detection as compare to existing methods. The NCARP considers the different layers parameters before classifying the vehicles either in legitimate node or malicious node. The MANEL and REALALERT based on just routing layer which is not sufficient especially for the high mobility networks. The next important performance is average throughput which is demonstrated in figure 4.

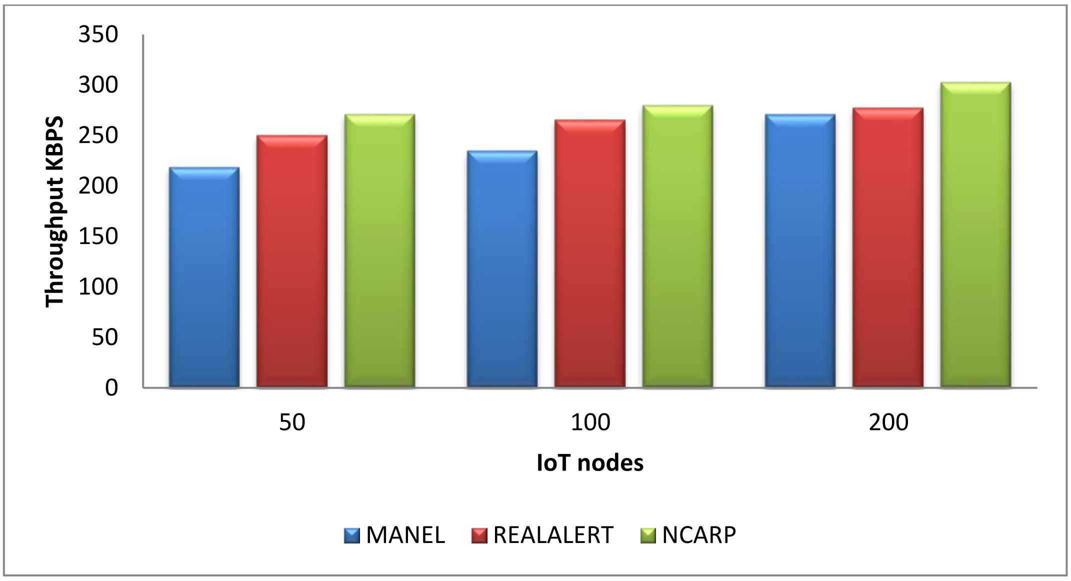

Figure 4. Performance analysis of average throughput

The throughput performance of MANEL is poor among all the three methods as it based on only the network layer cryptography solution to establish the secure communication among the nodes. The REALALERT computes the trust of the vehicles and then establish the path for data transmission at network layer, but in NCARP the cross-layer architecture assist to establish the more reliable and stable paths for data transmission in IoT enabled networks. The NCARP shows the improved throughput performance for each network. The routing overhead is another concern for the security methods in wireless communications. Figure 5 demonstrates the performance analysis of routing overhead. As observed in figure, as the number of nodes increasing the routing overhead increases. The more number of vehicles in network leads the extra burden of computing the nodes trust as well as cryptography operations while establishing the links. The NCARP performance outperformed the existing methods in routing overhead along with the precision, recall, average throughput, and routing overhead.

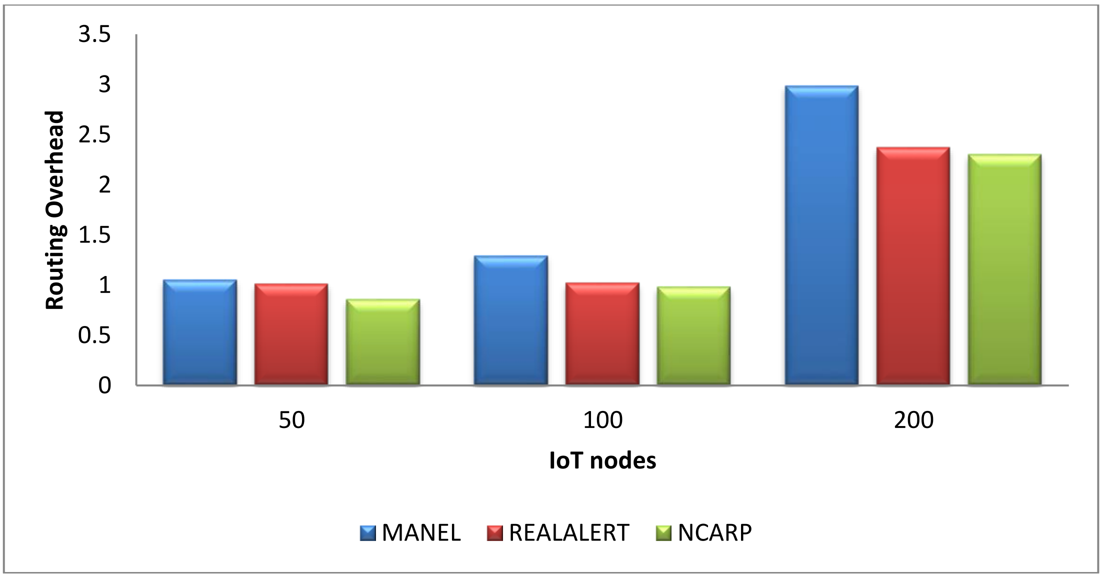

Figure 5. Performance analysis routing overhead

B. Attackers Variations

As observed in table 2, we investigate the performance of varying the number of attackers in network. The precision and recall rates performances observed in figures 6 and 7 respectively. As observed in figures, the precision rate and recall rates becomes less for the large number of attackers in network. The proposed NCARP achieved the better detection accuracy compared to both existing methods due the reasons disclosed in above section. Figures 8 and 9 demonstrate the outcomes of average throughput and routing overhead respectively. The proposed approach always delivered the optimized results under lower to higher number of attackers.

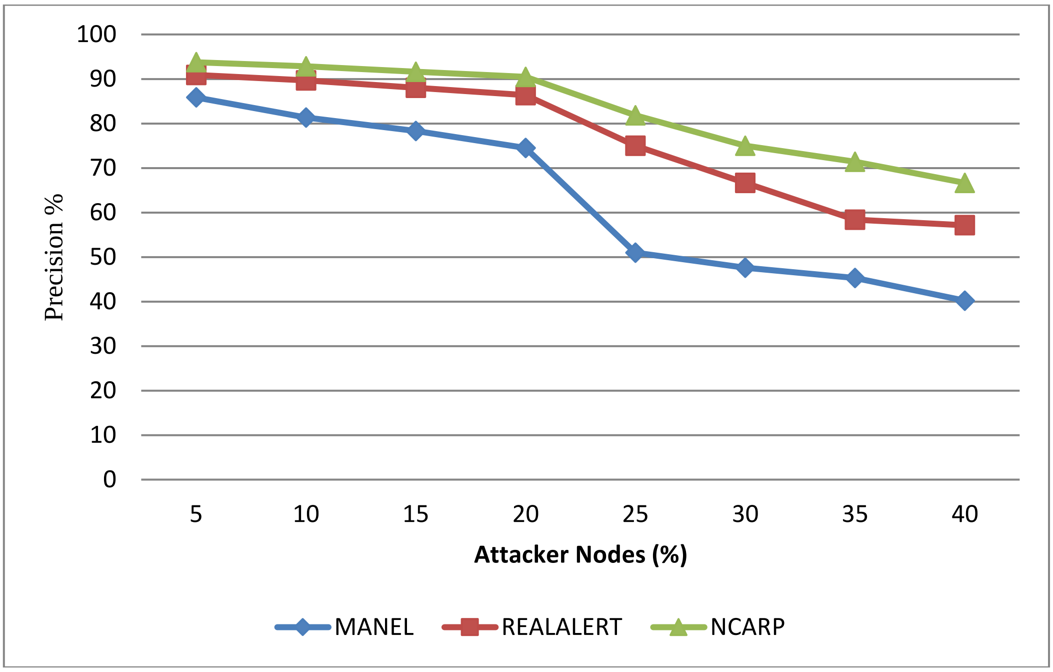

Figure 6. Precision Rate investigation

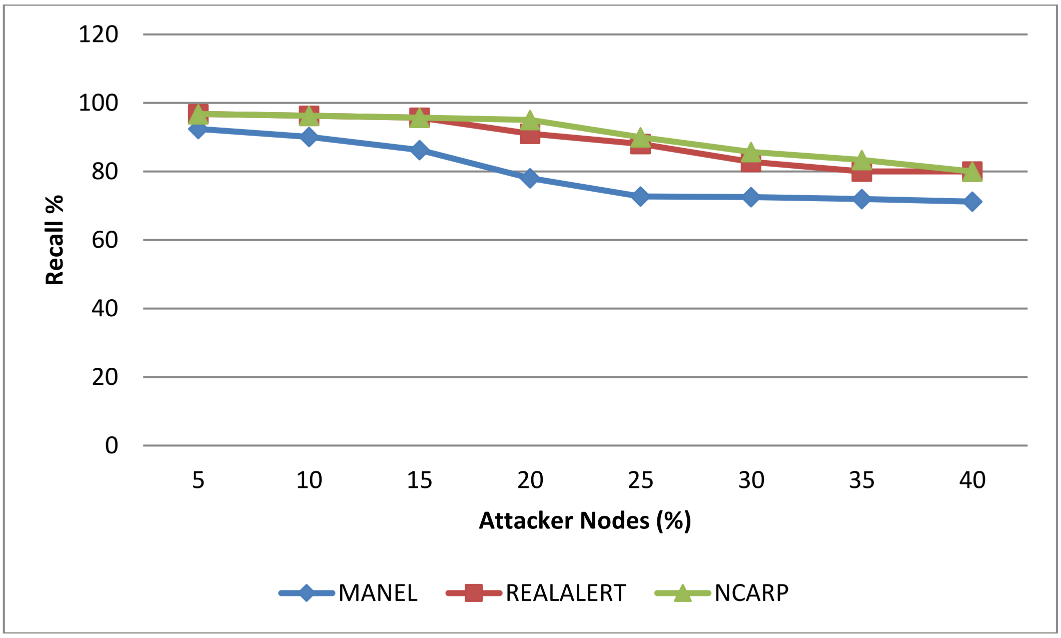

Figure 7. Recall Rate investigation

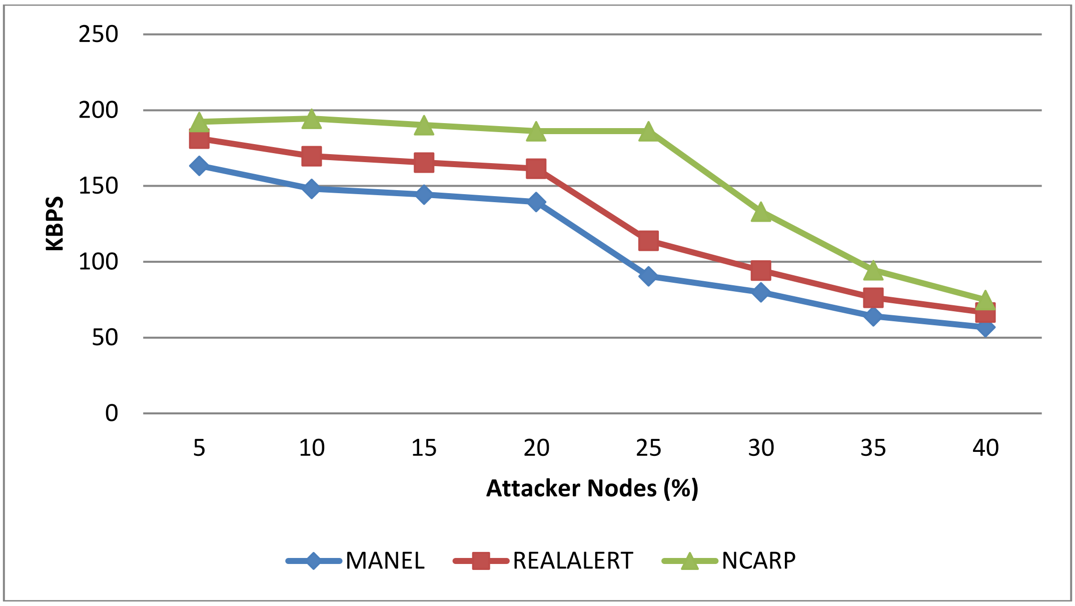

Figure 9. Average throughput investigation

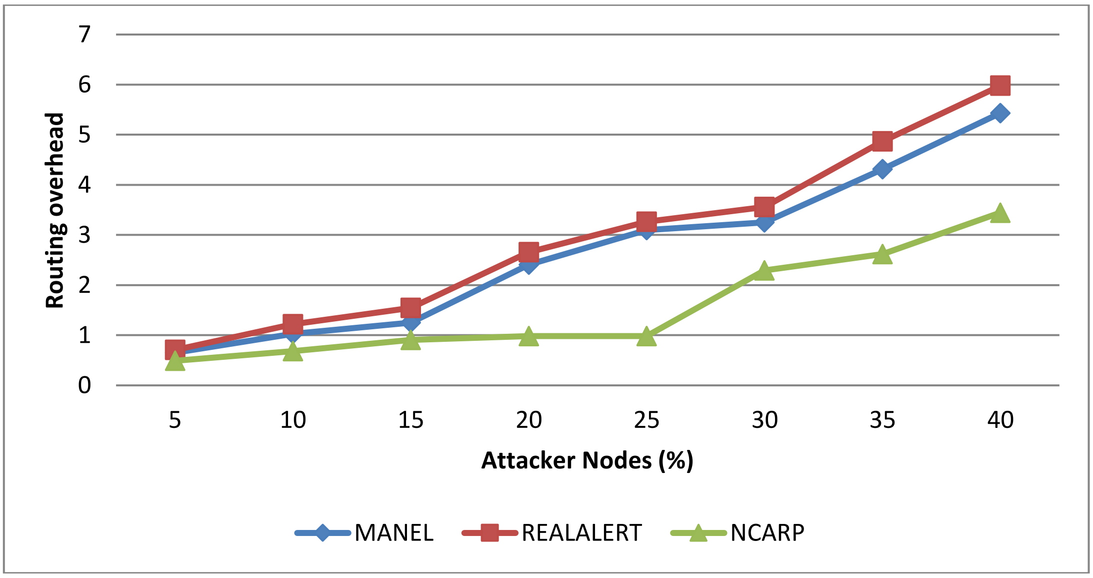

Figure 10. Routing overhead investigation

5. Conclusion and Future Work

For the IoT enabled wireless communications, the privacy preserving and secure communications is important research problems since from the last decade. In this work, we proposed the novel solution to secure the IoT enabled wireless communications based on higher mobility and network dynamics (e.g. VANET) using the NDN architecture rather than IP based networks and the trust based cross-layer architecture called NCARP. The design of NCARP presented in this paper which is further simulated and compared with the two recent solutions. The performance shows that NCARP achieved the significant improvement in malicious nodes detection and network QoS performance with minimum routing overhead. The future work we suggest is related to real time IoT based deployment of NCARP protocol.

6. References

[1] Atzori L, Iera A, Morabito G., "The internet of things: a survey", Computer networks, 54:2787–805, 2010.

[2] Zhao, K., Ge, L., "A survey on the internet of things security", In: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS). pp. 663–667, 2013

[3] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything", 2011

[4] Gubbi J, Buyya R, Marusic S, Palaniswami M., "Internet of Things (IoT): a vision, architectural elements, and future directions", Future Generation Computer System, 2013.

[5] Abdelaziz, A.K., Nafaa, M., Salim, G., "Survey of routing attacks and counter-measures", In: Proceedings of the 15th International Conference on Computer Modelling and Simulation (UKSim). 693–698, 2013.

[6] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," IEEE Internet of Things, Journal, 1(1):22–32, 2014.

[7] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M.W¨ahlisch. Information centric networking in the IoT: experiments with NDN in the wild. arXiv:1406.6608, 2014.

[8] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos, et al. Named data networking (NDN) project. NDN Technical Report NDN-0001, 2010.

[9] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro. Named data networking for IoT: an architectural perspective. In European Conference on Networks and Communications, 2014.

[10] S. K. Datta and C. Bonnet. Integrating named data networking in internet of things architecture. In IEEE Intl. Conference on Consumer Electronics-Taiwan, 2016.

[11] R. Ravindran, T. Biswas, X. Zhang, A. Chakraborti, and G. Wang. Information-centric networking based homenet. In IFIP/IEEE Intl. Symposium on Integrated Network Mgmt., 2013.

[12] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proc. 3rd ACM Int. Symp. MobiHocNetw. Comput.*, Lausanne, Switzerland, 2002, pp. 226–236.

[13] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Security*, Portoro˘z, Slovenia, 2002, pp. 107–121.

[14] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. 3rdAnnu. Int. Conf. Mobiquitous Syst. Workshops*, Jul. 2006, pp. 1–8.

[15] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in *Proc. 11th Int. Conf. MDM*, May 2010, pp. 112–121.

[16] S. Taha and X. Shen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 4, pp. 1665–1680, Dec. 2013.

[17] Z. Li, C. Liu, and C. Chigan, "On secure VANET-based ad dissemination with pragmatic cost and effect control," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 124–135, Mar. 2013.

[18] T. Chim, S. Yiu, L. Hui, and V. Li, "OPQ: OT-based private querying in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1413–1422, Dec. 2011.

[19] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[20] G. Rebolledo-Mendez, A. Reyes, S. Paszkowicz, M. Domingo, and L. Skrypchuk, “Developing a body sensor network to detect emotions during driving,” *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1850–1854, Aug. 2014.

[21] L.-Y. Yeh and Y.-C. Lin, “Aproxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1607–1621, Aug. 2014.

[22] P.L.R. Chze and K. S. Leong, "A Secure Multi-Hop Routing for IoT Communication," IEEE World Forum on Internet of Things (WF-IoT), pp. 428-432, 2014.

[23] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," presented at the Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, Budapest, Hungary, 2013.

[24] X. Anita, J. Martin Leo Manickam, and M. A. Bhagyaveni, "Two-Way Acknowledgment-Based Trust Framework for Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2013, p. 14, 2013.

[25] K.-F. Krentz, H. Rafiee, and C. Meinel, "6LoWPAN security: adding compromise resilience to the 802.15.4 security sublayer," presented at the Proceedings of the International Workshop on Adaptive Security, Zurich, Switzerland, 2013

[26] G. Mulligan, "The 6LoWPAN architecture," presented at the Proceedings of the 4th workshop on Embedded networked sensors, Cork, Ireland, 2007

[27] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, d. o. t. Akademinför innovation, et al., "Lithe: Lightweight Secure CoAP for the Internet of Things," IEEE Sensors Journal, vol. 13, pp. 3711-3720, 2013

[28] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN," Security and Communication Networks, vol. 7, pp. 2654-2668, 2014

[29] Indira Muhic, Migdat Hodzic “Internet of Things: Current Technological Review” PERIODICALS OF ENGINEERING AND NATURAL SCIENCES Vol. 2 No. 2 (2014)

[30] Wenjia Li, Member, IEEE, and Houbing Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 17, NO. 4, APRIL 2016

[31] ManelElleuchi, ManelBoujeleben, Mohamed Abid, “Securing RPL-Based Internet of Things applied for water pipeline monitoring”, 5th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2017

[32] Wenjia Li, Member, IEEE, and Houbing Song, Senior Member, IEEE, and FengZeng, "Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities", IEEE Internet of Things Journal (Volume: 5, Issue: 2, April 2018)

[33] Travis Mick, Reza Tourani, and SatyajayantMisra, “LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities,” IEEE Internet of Things Journal, 2017

[34] Md. Haidar Sharif, Ivan Despot, Sahin Uyaver “A Proof of Concept for Home Automation System with Implementation of the Internet of Things Standards” Periodicals of Engineering and Natural Sciences, Vol. 6, No. 1, April 2018, pp. 95 – 106.

[35] Hebah H. O. Nasereddin1, Moath Jehad Mohammad Faqir2 “The impact of internet of things on customer service: A preliminary study” Periodicals of Engineering and Natural Sciences Vol. 7, No. 1, June 2019, pp.148-155.

BIBLIOGRAPHY OF AUTHORS

Mr. Somnath B Thigale is Research Scholar at MUIT, Lucknow India, Hehas completed his B.E.CSE from Shivaji University, Kolhapur& M.E.CSE. from Solpaur university, Solapur.He is having more than 6 years Industry Experience and 7 years of Teaching experience for B.E &M.E.Students.He has certified Facilitor for IBM Rational,DB2 and Testing Technologies.Recently completed NPTEL certification in Introduction to Industry 4.0 and Industrial Internet of Things.His keen interest areas are Software Engineering,Software Testing, Internet of Things,Machine Learning.

Mr. Prakash R GadekarResearch Scholar at MUIT, Lucknow India.He did his B.Tech. and M.Tech. degree from Dr.BabasahebAmbedkar Technological University Lonere - Raigad.

Mr.VirendrakuamarA Dhotre is Research Scholar at MUIT, Lucknow India,.Hehas completed his B.E.CSE from Shivaji University,Kolhapur&M.tech.CSE.from Shivaji University, Kolhapur.He is having 1 years Industry Experience and 12 years of Teaching experience for B.E &M.E.Students.Recently completed NPTEL certification in Introduction to Industry 4.0 and Industrial Internet of Things.His keen interest areas are Internet of Things,Machine Learning.