International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 2, April 2021, pp. 1761∼1770
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i2.pp1761-1770

DEDA: An algorithm for early detection of topology attacks in the internet of things

Jalindar Karande, Sarang Joshi
Department of Computer Engineering, Pune Institute of Computer Technology, Savitribai Phule Pune University, Pune, India

Article Info

Article history:

Received Jan 3, 2020
Revised Jul 28, 2020
Accepted Aug 28, 2020

Keywords:

Distributed algorithm
Early detection
Internet of things
IoT security
Predictive detection
RPL
Topology attack

ABSTRACT

The internet of things (IoT) is used in domestic, industrial as well as mission-critical systems including homes, transports, power plants, industrial manufacturing and health-care applications. Security of data generated by such systems and IoT systems itself is very critical in such applications. Early detection of any attack targeting IoT system is necessary to minimize the damage. This paper reviews security attack detection methods for IoT Infrastructure presented in the state-of-the-art. One of the major entry points for attacks in IoT system is topology exploitation. This paper proposes a distributed algorithm for early detection of such attacks with the help of predictive descriptor tables. This paper also presents feature selection from topology control packet fields. The performance of the proposed algorithm is evaluated using an extensive simulation carried out in OMNeT++. Performance parameter includes accuracy and time required for detection. Simulation results presented in this paper show that the proposed algorithm is effective in detecting attacks ahead in time.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Jalindar Karande
Research Scholar, Department of Computer Engineering
Pune Institute of Computer Technology, Pune, India
Email: jalindar.karande@ieee.org

1. INTRODUCTION

The internet of things (IoT) has made possible seamless communication between machines and human. IoT systems ability of continuous data collection, seamless communication, autonomous decision making and ability to control the physical world by implementing decisions changed operational paradigms of many operational systems. IoT made it possible to replace human in many critical tasks. These resulted in minimizing human errors and increased the productivity of the systems. Now, internet of things (IoT) has become a vitally important application in every business domain including but not limited to smart home, smart city, smart grid, connected cars, connected healthcare, industrial automation, precision farming, smart wearables, retail and supply chain management. Even in the COVID-19 outbreak millions of population are locked down to home but IoT systems were still on the field. IoT systems made it possible to keep critical infrastructures functioning through remote monitoring and controlling. IoT systems were extensively used during COVID-19 outbreak for pandemic management. These application includes the use of smart wearables to real-time monitoring of health data as well as compliance with home quarantine, real-time data collection through IoT thermometers, remote instructions and application of IoT enabled robots to serve patients and to maintain hospital hygiene. The detailed survey of IoT applications during COVID-19 outbreak is presented in [1].

IoT security is a growing concern, given that various critical infrastructures and applications are di-

rectly connected and controlled using IoT. These concerns include security of data, connected infrastructure, human as well as IoT infrastructure itself. The security breach of the IoT system may lead to exploiting critical infrastructure and may put many lives at stake. IoT systems are connected to the physical world in a more concrete way than conventional computer systems. This makes a breach of security of IoT system more catastrophic in nature. This raise concerns over using conventional security algorithms for detection of security attacks in IoT systems. Security requirements of IoT embedded into critical infrastructures are analysed in [2], which also highlights that conventional internet security approaches are not enough to address the security of IoT systems used for management of critical infrastructures. Security concerns of use of IoT in industrial applications are highlighted in [3, 4]. Analysis of security attack detection mechanisms in an industrial setting is presented in [5] along with a review of different commercial tools available for attack detection. Authors highlighted the need for more focused solutions for the protection of industrial IoT systems. The not only breach of IoT systems security leads to attack on IoT systems but compromised IoT devices are used to enable large scale attacks on other critical infrastructures. A detailed assessment of such IoT enabled attacks is presented in [6].

Many techniques have been proposed in the state-of-the-art for preventing security attacks on IoT devices which includes authentication [7, 8], Access control [9] and data encryption [10] for IoT. Although several measures have been taken to prevent security attacks on IoT systems, the low compute power of IoT devices still makes it vulnerable to attacks. The vulnerability assessment of consumer IoT devices presented in [11] shows that around 10% devices are prone to at least one critical risk vulnerability, 40% devices had at least one high-risk vulnerability, and 68% devices had at least one medium risk vulnerability and 42% devices had at least one low-risk vulnerability. These vulnerable consumer devices analyzed in [11] include smart TV, webcam and printers from a wide range of manufacturers. These highlights that security attack detection is of critical importance even though prevention mechanism is present into IoT devices.

IoT devices use RPL protocol for building network topology to connect to the Internet. The detailed working of the RPL protocol is presented in [12]. RPL protocol is prone to be exploited and becomes an entry point for many attacks on IoT devices. Security of RPL protocol is still an open problem [13]. The resource-constrained nature of IoT devices, the possibility of bypass of preventive mechanism and probable catastrophic loss due to breach of security of IoT devices motivated authors to design of an algorithm for early detection of such security attacks without putting heavy resource load on individual IoT device. The proposed algorithm is distributed in nature and will run in two phases. The first phase involves collecting and building descriptive tables locally, whereas the second phase involves exchanging descriptive tables and concluding the presence of an attacker. The main contribution of this paper are summarized follows:

– This paper presents a comprehensive review of the-state-of-the-art for detection of IoT security attacks
– This paper presents the selection of control packet parameters for attack detection
– This paper presents a distributed algorithm for early detection of security attacks on IoT devices
– This paper presents a performance evaluation of the proposed algorithm in early detecting attacks

Next section presents a review of the state-of-the-art for security attacks and countermeasures on the IoT system. Section 4 proposes distributed algorithm for early detection of security attacks through the use of predictive descriptor tables. Section 5 presents the result analysis to assess the effectiveness of the proposed algorithm for the early detection of security attacks.

2. LITERATURE REVIEW

Identifying and mitigating attackers from the networked system has been the topic of importance. Several methods and algorithms have been proposed in the state of the art to detect specific attacks. Networked systems may be the target of multiple attacks. We need a mechanism to integrate several attack detection methods into a single framework. Standardised framework for such detection system called CIDF [14] is presented by a working group created by DARPA now called intrusion detection working group (IDWG). Snort [15] is one the proven open-source attack detection tool, but the feasibility of deploying a snort system in IoT nodes is argued in [16] due to resource constraints on IoT nodes. Behaviour-based analysis of vulnerabilities of the drone-based IoT system along with detection of vulnerability using Petri net is presented in [17]. Attackers exploit vulnerabilities in IoT devices and protocols to enter into the IoT networks. The approach based on the modelling relationship between vulnerabilities as a graph and using a graph-theoretic approach for detecting attack is presented in [18].

Various attacks against RPL protocol have been demonstrated in [19] along with Lightweight Heartbeat algorithm to detect attackers. The proposed algorithm is relying only on IPsec with ESP communication and in many cases, IPsec protocol might not be deployed in IoT nodes. This algorithm is also creating additional workload for resource-constrained IoT nodes. A comprehensive review of security challenges in IoT topology is presented in [20]. This paper further analysed IoT protocols, including RPL and 6LoWPAN for potential security weakness along with the need for further research in IoT topology security. The specification-based method for identifying RPL topology attacks on the IoT system is presented in [21]. This method builds a finite state machine for RPL topology operations. Topology control information (DIO packets) throughout the system is monitored by monitoring nodes and information within these packets is used for state transitions. The approach presented in the paper is effective to detect more complex attack scenarios like multiple and collaborative attacks.

Within the multi-hop IoT system, discovering and establishing the route to the gateway node is one of the crucial tasks. The efficiency of this task leads to performance improvement in the overall IoT system. This task is executed in a distributed manner in IoT protocols to take care of runtime link failures or new additions of nodes in the system. Unfortunately, this crucial distributed task becomes the target of the attack. Such concern of security of route discovery has been presented in terms of MANET [22], which applies to IoT systems also as it shares characteristics like mobile nodes and ad-hoc nature with MANET. This paper also highlights preventing such attack is very costly and almost impossible in given situations and more focus should be given on detection of attack than prevention of it.

Intrusion detection in IoT trough traffic filtering is presented in [23]. This work also highlights several open challenges in attack detection using traffic filtering which includes complex traffic characterization, difficulties in preparing the blacklist and the white list for traffic filtration, traffic sampling, building realistic attack models and the impact of false positives. Deep packet inspection based attack detection mechanism is presented in [24]. This mechanism makes use of the regular expression in terms of DFA to represent the rule. Representation of rules in regular expression makes it easy to implement in the hardware through field programmable gate arrays (FPGAs) which make it faster than software approaches. The number of states required to represent all possible attack signatures is very large and there are always chances of changing the signature in new attacks.

A review of machine learning-based approaches for enhancing the security of the IoT system is presented in [25]. These approaches include authentication based on a prediction of communication parameters, machine learning algorithms for access control, secure offloading and machine learning-based attack detection methods. This paper further concluded that machine learning needs intensive computing power and high communication overhead. Also, the need for a large amount of training data and the complex feature extraction process makes these algorithms unappealing for resource-constrained devices. Machine learning-based mechanism using inferencing and predicting states of the system is presented in [26] to detect anomalies and attacks in the IoT system. Random neural network-based approach for detection of attackers in IoT systems is presented in [27]. This approach learns anomalies in the performance of the system using the random neural network and relates it to the failure of IoT node or attacker's presence. A game theory-based approach is for attack detection along with a reputation model is presented in [28], which is capable of detecting various attacks on IoT systems. Attack detection mechanisms are traditionally evaluated using either test dataset or generating attacks manually. This approach gives better result in the evaluation phase but may fail to detect the real attack. Genetic programming-based approach for generating test attacks used for evaluating the accuracy of the detection mechanism is presented in [29]. Deep learning-based approach for attack detection in IoT is presented in [30]. A framework for DDoS attack detection in IoT systems based on cosine similarities within the traffic flow is presented in [31].

The artificial neural network-based architecture for detection of DDoS/DoS attack is presented in [32]. This architecture makes use of both forward and backward learning mechanisms to train and identify malicious traffic. Hidden Markov model-based classifier is proposed in [33] to detect anomalies in the data, which is used to alert about the security attack. This method makes use of multiple knowledge domains like knowledge of the physical process and the control system to identify the attack. This approach is suitable for implementation in an industrial control system, but may not be suitable for resource-constrained IoT systems. Game theory-based approaches for detection of the attacker makes use of conflicting goals of attackers and detection engines. A two-player game theory-based approach where the attacker and detection engine are opponents is presented in [34] to collaboratively detect security attacks in IoT systems.

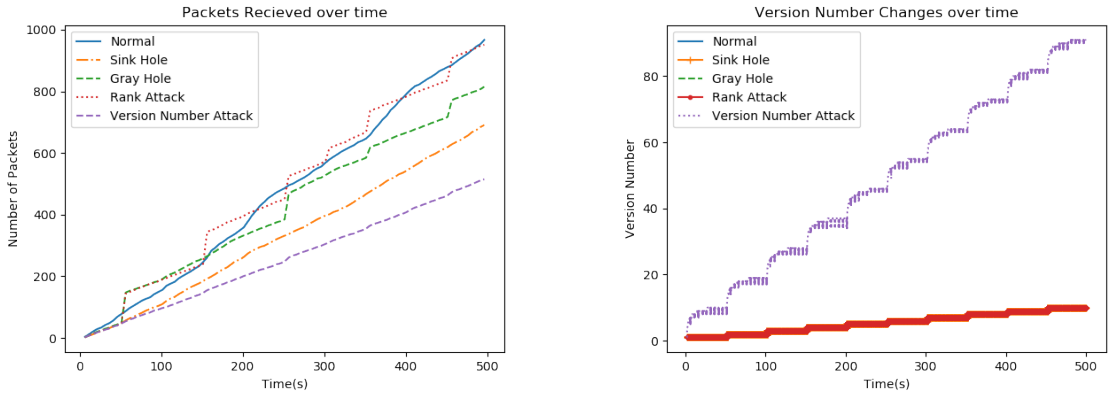
The distributed attack detection method with monitoring the communication pattern of nearby nodes and identifies suspicious communication is presented in Kinesis [35]. In this method, identified suspicious communication in two hops distance is reported to the central detection node. The central node is responsible for taking the final decision about the suspicious node and notifies its decision to all other nodes in the system. This mechanism puts additional overhead of maintaining the two-hop communication log. The effectiveness of the mechanism is affected by fabricated communication patterns of cooperative attackers. Another distributed algorithm for detection of the security breach called version number attack is presented in [36]. This method of attacker identification makes use of placement of additional nodes dedicated to monitoring network communication, which results in the higher cost. Further, this approach is not effective in the case of multiples cooperative attackers exploiting the IoT system.

The model for distributed detection of the security attack on the IoT system is presented in [37] along with proof of the concept implementation, which make use of fog computing nodes to deploy extreme learning machine based mechanism for attack detection at local. Further security state information collected from fog computing nodes is summarised at the cloud node to predict the future course of action of the attacker. Various security attacks over RPL based IoT networks have been demonstrated in [38]. The paper also evaluated various attack detection mechanism in different attack scenario like a single attacker, multiple attackers and collaborative attacks. This paper highlighted the need for designing the security detection mechanism for early detection of attacks and include capabilities of detecting collaborative attacks.

3. IDENTIFICATION OF FEATUTES FOR ATTACK DETECTION

Through the comparative analysis of simulation tools used for IoT research presented in [39], OMNeT++, a discrete event simulation tool, is used for the simulation study. Objectives of simulation study include finding out effective features for attack detection, the effectiveness of predicting values of features in future and accuracy of detection mechanism. The IoT system is simulated in OMNeT++ with the implementation of RPL at the network layer and IEEE 802.15.4 standard at the physical layer and MAC layer.

Figure 1 shows a comparison of the total number of data packets received at the gateway node with time during various attacks scenarios. The results show that there is a drastic increase in packet loss in the IoT system during attacks. Version number attack demonstrates the worst performance with huge packet loss. The presented results show a periodic steep increase in the number of packets received in the system under attack. This steep increase is the result of the periodic global repair of network topology i.e DODAG in RPL Protocol. The results show that deviation in throughput changes is a good feature to be considered for attack detection. Figure 1 demonstrates the increase in the DODAG version number during different attack scenarios. Demonstrated a high increase in the version number indicates frequent topology reformation triggered by malicious nodes. This result motivates to use the rate of change of the version number of DODAG as a feature to identify the presence of the version number attacker in the IoT system.



(a) (b)

Figure 1. (a) Throughput changes (b) DODAG version number

Figure 2 shows changes in the rank distribution over time. It indicates that the rank value tends to shrink in rank attack and tends to elevate in case of version number attack. This deviation in the distribution of

the rank is a good feature to be used for detecting the presence of an attacker in the IoT system. Figure 2 also shows the difference between the standard deviation of the rank value of DODAG for different scenarios over time. This differences will be useful for identifying the attacker in RPL based IoT network. Figure 2 shows that during normal operation, the rank of a node is increasing with distance from the gateway node. Whereas in case of attack scenarios, nodes far from gateway node also tend to falsely get lower rank value. Figure 3 shows deviation in DIO packets received and DAO packets received respectively in different scenarios. This variation in values of different parameters during various attack scenarios will be useful as features for the detection of the attacker in the IoT system.

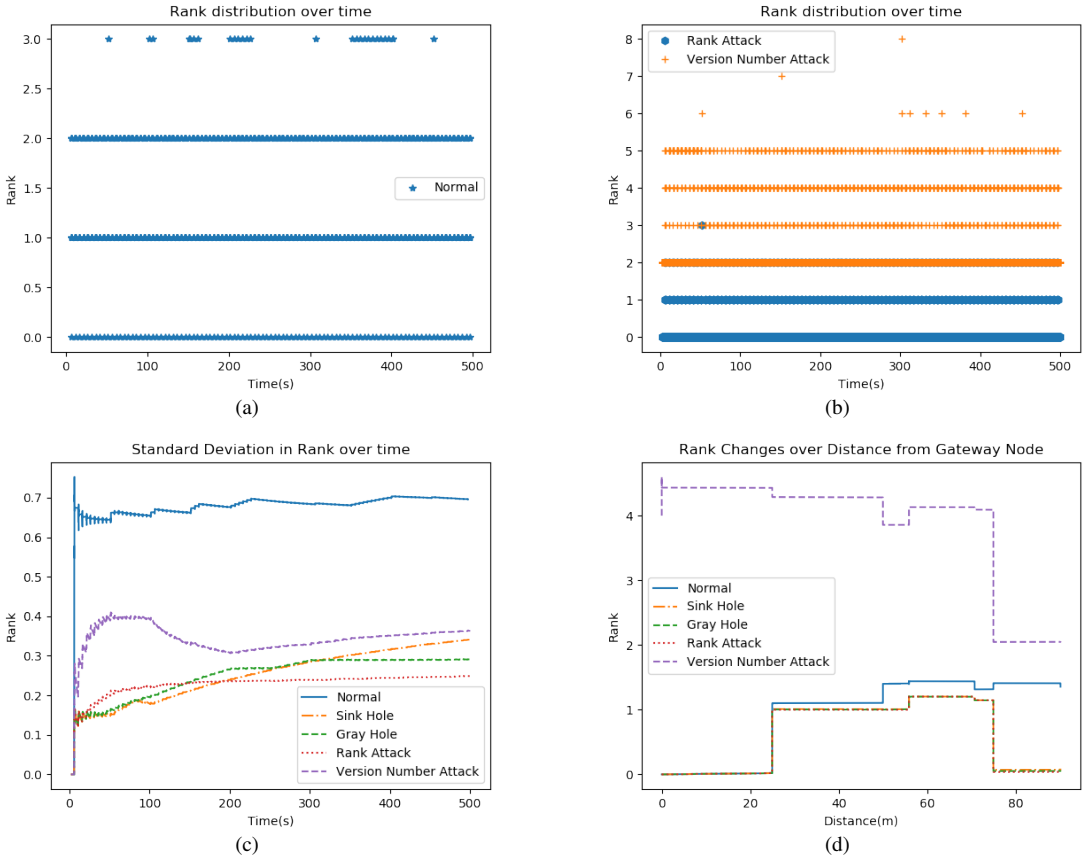


Figure 2. (a) Distribution of rank (without attack), (b) Distribution of rank (attack), (c) Standard deviation of Rank, (d) Rank vs distance from gateway node

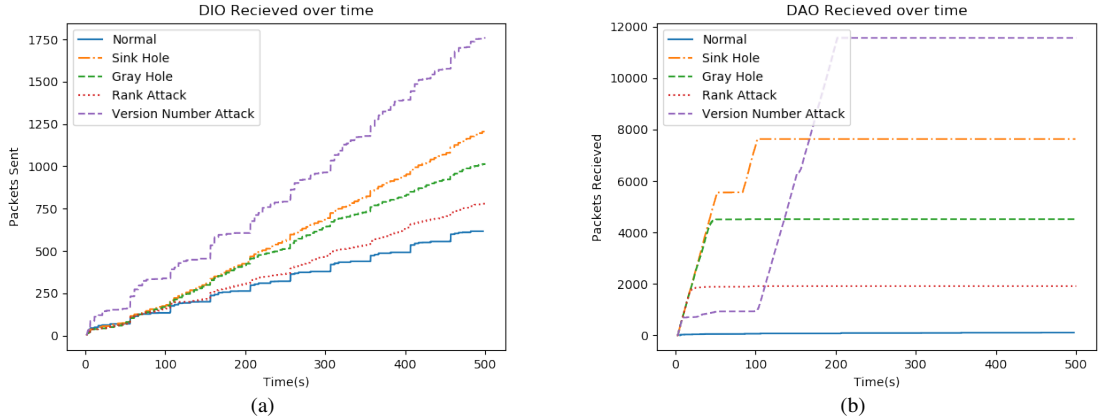


Figure 3. (a) DIO packets received, (b) DAO packets received

4. PROPOSED ALGORITHM

The proposed algorithm, DEDA for topology attack detection in the IoT network will work by the placing monitoring nodes in addition to normal nodes for attack detection. The placement of additional nodes will result in the uninterrupted operation of ordinary nodes by avoiding computing and memory overload of executing detection algorithms on them. These additional monitoring nodes will monitor all traffic from nearby IoT nodes and build a descriptor table of it. This descriptor table will include a count of various control packets transmitted from the individual node. This descriptor table will also include information about network parameters like rank, version number etc. sent in control packets by individual nodes. Every monitoring node is preparing a partial descriptor table and also making a log of changes in the partial descriptor table. This log of changes and current values is used to predict the descriptor table early in time. The predicted descriptor table is shared with other monitoring nodes. Every monitoring aggregate values in the descriptor table received from other monitoring nodes. This aggregation of the predicted descriptor table will give a birds-eye view of the current state of the system to every monitoring node. Monitoring nodes make use of the predicted descriptor table to detect the presence of the attacker and identifies which node is the attacker along with the type of attack being launched. Information about identified attacker is propagated to other nodes for necessary actions and precautions. The detailed working of the algorithm is presented in Algorithm 1 and Algorithm 2

Algorithm 1: DEDA: Distributed Early Detection Algorithm Phase-I

```
RankTuples = ∅;
VersionNumberTuples = ∅;
DISRec = DIORec = DAORec = DAOARec = ∅;
localRouteTable = ∅;
n= number of IoT nodes in the system;
i=0;
while i < n do
    DISRec[i] = DIORec[i] = DAORec[i] = DAOARec[i] = 0;
end
listen to network trafiic;
if control packet then
    source=source address from base packet;
    dest=destination address from base packet;
    if DIO packet then
        RankTuples = RankTuples ∪ (source, rank in DIO);
        VersionNumberTuples = VersionNumberTuples ∪ (source, versionNumber in DIO);
        DIORec[getIndex(source)] ++ ;
    else
        if DAO packet then
            localRouteTable = localRouteTable ∪ (source, destination);
            DAORec[getIndex(source)] ++ ;
        else
            if DAOA packet then
                localRouteTable = localRouteTable ∪ (destination,source);
                DAOARec[getIndex(source)] ++ ;
            else
                DISRec[getIndex(source)] ++ ;
            end
        end
    end
end
PD = (RankTuples,VersionNumberTuples,DISRec,DIORec,DAORec,DAOARec,localRouteTable);
PPD = predict using timeseries pattern(partial descriptor table);
broadcast predicted PPD;
```

Algorithm 2: DEDA: Distributed Early Detection Algorithm Phase-II

```
Descriptor Table = ∅;
i=0; n= number of PPD received;
while i < n do
    Descriptor Table = Descriptor Table ∪ PPD[i];
end
i=0; n= number of nodes in the IoT system;
while i < n do
    isAttacker = Detect using machine learning model(Descriptor Table, i);
    if isAttacker then
        Announce to all nearby nodes;
    else
        Ignore;
    end
end
```

4.1. Mathematical model of proposed system

Let D as a set of descriptor tables $\{D_1, D_2, \ldots, D_n\}$ where n is the total number of monitoring nodes and D_i, the descriptor table of i^{th} monitoring node. D_i is set of tuples F as $Di = \{F_{i1}, F_{i2}, \ldots, F_{im}\}$, where m is the number of nodes monitored by i^{th} monitoring node. Let F_{ij} is the set of features of j_{th} IoT node monitored by i_{th} monitoring node as $F_{ij} = \{f_{ij1}, f_{ij2}, \ldots, f_{ijl}\}$, where l is $|Fij|$

Let L is the set of log tables $\{L_1, L_2, \ldots, L_n\}$, where n is the total number of Monitoring nodes and L_i is the log maintained by i_{th} monitoring node, as $L_i = \{D_{it}, D_{it-1}, \ldots, D_{it-r}\}$, where r is the number of past descriptor tables L_i and D_{it} indicates snapshot of D_i at time t.

Let W_i is the set of weights of i_{th} descriptor table as $W_i = \{w_1, w_2, \ldots, w_l\}$, where l is $|F|$

Let PD as the set of predicted descriptor tables $\{PD_1, PD_2, \ldots, PD_n\}$, where n is the total number of monitoring nodes and PD_i as the predicted descriptor table of i_{th} monitoring node.

Value of the predicted features f at time t is calculated using,

$$f_t = \sum_{i=0}^{l} \sum_{j=0}^{n} (f_j * W_i j) \tag{1}$$

where l indicates the number of past descriptor tables and n indicates the number of features.

5. RESULT ANALYSIS

Accuracy of predicting rank of the node and version number of the node in the future based on the history of values present into the descriptive table is presented in Figures 4(a) and (b) (see in appendix) respectively. Features other than the rank and the version number are more predictable and average accuracy of prediction is shown in Figure 4(c) (see in appendix). Results also show that we need to keep the history of descriptive tables and a length of the history table has an impact on the accuracy of prediction. It is also evident that keeping a very long history in not required as accuracy is soon coming to the saturation point. We need to use predicted features for early detection of attacks on IoT resources. Figure 4(d) (see in appendix) shows the accuracy of detecting the attacker ahead in time. The accuracy of predicting long ahead is less and tradeoff between the accuracy and the time ahead has to be decided in the deployment of the proposed solution.

6. CONCLUSION

The proposed algorithm works in two parts in parallel, where phase-I builds local descriptor table and phase-II builds a global descriptor table and detects the presence of the attacker. The predicted local descriptor holds future values of fields present in the control packet. This use of future values by attack detection model results in detection of attack in an early stage. The effectiveness of detecting attack early is proved through the extensive simulation study. The proposed algorithm will be very helpful in the early detection of attacks and minimize damage in IoT systems. Limitations of the proposed algorithm include the additional cost of putting

monitoring nodes and incapable of detecting unknown attacks. Our future work includes designing a predictive algorithm for early detection of collaborative attacks and evaluating its effectiveness.

APPENDIX

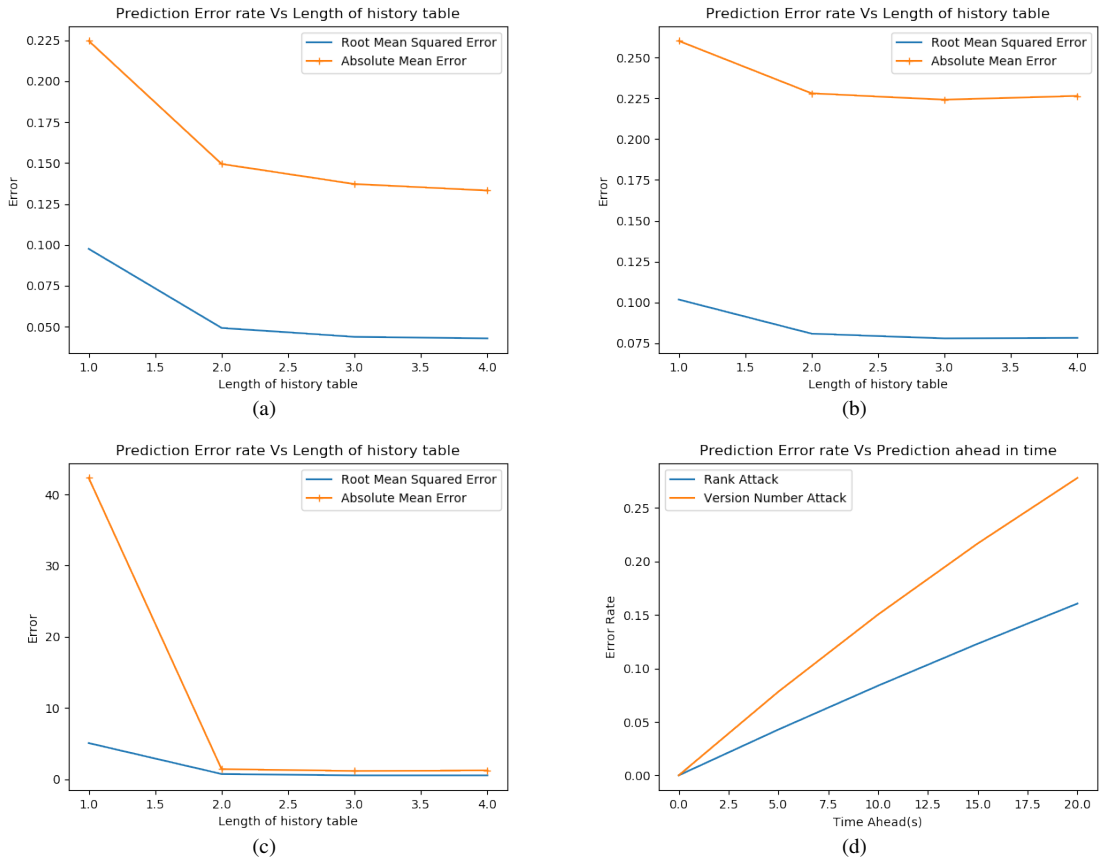


Figure 4. Prediction accuracy, (a) Rank prediction accuracy, (b) Version number prediction accuracy, (c) Average prediction accuracy of all features, (d) Accuracy of attack detection

REFERENCES

[1] R. P. Singh, M. Javaid, A. Haleem, and R. Suman, "Internet of things (IoT) applications to fight against covid-19 pandemic," *Diabetes and Metabolic Syndrome: Clinical Research and Reviews*, 2020.

[2] J. Jenkins and M. Burmester, "Runtime integrity for cyber-physical infrastructures," *International Conference on Critical Infrastructure Protection*, pp. 153-167, 2015.

[3] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based scada systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375-1384, 2016.

[4] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *computers and security*, vol. 56, pp. 1-27, 2016.

[5] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Analysis of intrusion detection systems in industrial ecosystems," *14th International Conference on Security and Cryptography (SECRYPT 2017)*, 2017.

[6] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys and Tutorials*, pp. 3453-3495, 2018.

[7] A.-T. Fadi and D. B. David, "Seamless authentication: For IoT-big data technologies in smart industrial application systems," *IEEE Transactions on Industrial Informatics*, 2020.

[8] Q. Liu, B. Gong, and Z. Ning, "Research on clpkc-idpkc cross-domain identity authentication for IoT environment," *Computer Communications*, 2020.
[9] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567-592, 2019.
[10] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, 2019.
[11] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer internet of things (IoT) devices: A scalable approach," *IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 179-181, 2017.
[12] T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, R. K. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks," *RFC*, vol. 6550, pp. 1-157, 2012.
[13] A. Arena, P. Perazzo, C. Vallati, G. Dini, and G. Anastasi, "Evaluating and improving the scalability of RPL security in the internet of things," *Computer Communications*, vol. 151, pp. 119-132, 2020.
[14] C. ord Kahn, P. A. Porras, S. Staniford-Chen, and B. Tung, "A common intrusion detection framework," *Journal of Computer Security,* 1998.
[15] M. Roesch, "SNORT: Lightweight intrusion detection for networks," *Lisa*, vol. 99, no. 1, pp. 229-238, 1999.
[16] A. Sforzin, F. G. Mármol, M. Conti, and J.-M. Bohli, "RPIDS: Raspberry pi ids-a fruitful intrusion detection system for IoT," *2016 Intl IEEE Conferences on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld*, pp. 440-448, 2016.
[17] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerability assessment of drones-enabled industrial internet of things (IIoT)," *IEEE Access*, vol. 6, pp. 43368-43383, 2018.
[18] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586-43601, 2018.
[19] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 2013.
[20] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for Internet of things: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 198-213, 2016.
[21] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing RPL from topology attacks," *Wireless Days (WD),* pp. 1-3, 2011.
[22] M. Burmester and B. De Medeiros, "On the security of route discovery in MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1180-1188, 2009.
[23] W. Meng, "Intrusion detection in the era of IoT: Building trust via traffic filtering and sampling," *Computer*, vol. 51, no. 7, pp. 36-43, 2018.
[24] F. Yu, Z. Chen, Y. Diao, T. Lakshman, and R. H. Katz, "Fast and memory-efficient regular expression matching for deep packet inspection," *Proceedings of the 2006 ACM/IEEE symposium on Architecture for networking and communications systems,* pp. 93–102, 2006.
[25] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning," *arXiv preprint arXiv:1801.06275*, 2018.
[26] N. Muralidhar, C. Wang, N. Self, M. Momtazpour, K. Nakayama, R. Sharma, and N. Ramakrishnan, "ILLIAD: Intelligent invariant and anomaly detection in cyber-physical systems," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 9, no. 3, pp. 1-20, 2018.
[27] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent intrusion detection in low-power IoTs," *ACM Transactions on Internet Technology*, vol. 16, no. 4, pp. 1-25, 2016.
[28] H. Sedjelmaci, S. m. Senouci, and T. Taleb, "An accurate security game for low-resource IoT devices," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1-1, 2017.
[29] K. Mrugala, N. Tuptuk, and S. Hailes, "Evolving attackers against wireless sensor networks using genetic programming," *IET Wireless Sensor Systems*, vol. 7, no. 4, pp. 113-122, 2017.
[30] A. Abeshu and N. Chilamkurti, "Deep learning: the frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169-175, 2018.

[31] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-IoT networks," *IEEE access*, vol. 6, pp. 15941-15957, 2018.
[32] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of IoT networks using artificial neural network intrusion detection system," *2016 International Symposium on Networks, Computers and Communications (ISNCC),* pp. 1-6, 2016.
[33] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345-1360, 2015.
[34] H. Wu and W. Wang, "A game theory based collaborative security detection method for Internet of things systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1432-1445, 2018.
[35] D. Midi, S. Sultana, and E. Bertino, "A system for response and prevention of security incidents in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 13, no. 1, pp. 1-38, 2016.
[36] A. Mayzaud, R. Badonnel, and I. Chrisment, "A distributed monitoring strategy for detecting version number attacks in RPL-based networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472-486, 2017.
[37] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291-298, 2018.
[38] J. Karande and S. Joshi, "Comprehensive assessment of security attack detection algorithms in Internet of things,"*2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA),* pp. 1-6, 2018.
[39] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of things (IoT): Research, simulators, and testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637-1647, 2017.

BIOGRAPHIES OF AUTHORS

Jalindar Karande received Masters in Computer Science and Engineering and Bachelors in Information Technology from the University of Pune. He is currently a research scholar in the Department of Computer Engineering, Pune Institute of Computer Technology, Savitribai Phule Pune University, Pune, India. He is Google Cloud Platform Certified Professional Data Engineer and also holds a license from Databricks for Spark. His research interests include IoT, Big Data and Machine Learning. He has published several papers in Journals and reputed conferences in these areas. He is affiliated with IEEE as Graduate Student member.

Prof. Sarang Joshi received a PhD in Computer Science and Engineering from Bharati Vidyapeeth, Pune, India. He received a Masters in Computer Engineering and a Bachelors in Computer Engineering from University of Pune, India. He is currently a Professor in Department of Computer Engineering, Pune Institute of Computer Technology, Savitribai Phule Pune University, Pune, India. He has 30 years of teaching experience. His research interests include Algorithms, Intelligence, IoT, Big Data and Machine Learning. He has guided several research scholars and published several papers in reputed Journals and Conference Proceedings in these areas. He has previously served as Chairman, Board of Studies of Computer Engineering at Savitribai Phule Pune University. He has authored books on "Big Data Mining - Application Perspective" and "Design and Analysis of Algorithms".