Jestr

Journal of Engineering Science and Technology Review 14 (1) (2021) 38 - 45

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

Direct Neighbour Sink Reputed Trust Based Intrusion Detection System to Mitigate Sinkhole Attack in RPL for IoT Networks

Bimal Patel* and Parth Shah

Chandubhai S. Patel Institute of Technology (CSPIT), Faculty of Technology & Engineering (FTE), Charotar University of Science and Technology (CHARUSAT), Changa, Gujarat, India

Received 24 December 2020; Accepted 18 February 2021

Abstract

In terms of heterogeneous devices and sensors, man and machine collaborate seamlessly, giving birth to the Internet of People, Internet of Things, and Internet of the Future. IoT combines the power of IPv6 for network connectivity, sensing and nextgen communication technologies to meet future demands. Internet Engineering Task Force (IETF) came up with a concept of 6LoWPAN possessing characteristics like low power, bandwidth and cost. To bridge the routing gap and to collaborate between low power private area network and the outside world, IETF ROLL group proposed IPv6 based lightweight standard RPL (Routing protocol for low power and lossy networks). As an essential component of 5G communication, the IoT environment is more susceptible to various routing attacks due to constraint resources, complex infrastructure and heterogeneity of smart things. In our work, we have explored sinkhole attack which disrupts routing paths and silently drop packets degrading the overall quality of service parameters. Our work proposed Direct Neighbor Sink Reputed Trust Based Intrusion Detection System (DSTIDS) to mitigate the effect of a sinkhole attack. The experimental evaluation is performed and analyzed using Contiki 3.0 operating system along with inbuilt simulator cooja. Our proposed scheme DSTIDS shows much better performance in terms of various metrics like packet delivery ratio, detection rate, false negative rate and false positive rate compared to other state of the art existing schemes for sinkhole attack.

Keywords: IoT, 6LoWPAN, RPL, Sinkhole Attack, DSTIDS, Contiki 3.0, Cooja

1. Introduction

Ever growing networks of physical object that tends to interconnect the real world with a digital concept in the form of smartness are gaining momentum. This gives emergence to the term Internet of Things (IoT) proposed by Kevin Aston. According to Gartner report Internet of things installed base will be populated by 50 billion smart devices[1]. Anything communication is now widespread to Internet of People, Internet of Content and Internet of Services with the help of IPv6 addressing. IoT enabled device will provide a smart application to the industry in the form of Industrial IoT, agriculture, smart home, healthcare, logistics etc. Wireless sensor networks, actuators and embedded system with microcontroller and chips acting as an integral part in designing smart and intelligent devices[2],[3]. Due to various challenges in terms of heterogeneity, scalability, complex infrastructure, security and limited resource constraint environment in the form of memory and computational power, there has been a great deal of interest from researchers around the globe in IoT security, and most IoT systems have vulnerabilities that could allow an attacker to gain control over IoT devices. As shown in Figure 1 indicated by a white paper published by [4] amount of things connected to the internet has exceeded the amount of people living on earth.To bridge the routing gap and to collaborate between low power private area network and the outside world, IETF ROLL group proposed IPv6 based lightweight standard RPL (Routing protocol for low power and lossy networks)[5]–[7]. Due to constraint resources, heterogeneous smart things and lossy network IoT environment are prone to routing attacks. Sinkhole attack is discussed, compared and simulated later. If these attack is not detected, there can be considerable consequences in terms of quality of service parameter. As security of data is at the stack and routing information is a crucial factor influencing connectivity and performance of data exchange, this is one of the reason to detect and mitigate attacks and provide trust based solutions.

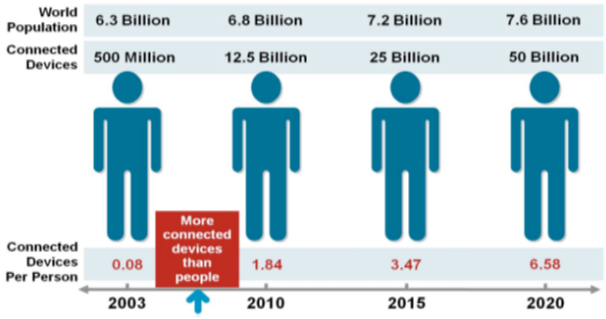

Fig. 1. Sizing the opportunity

Since standard routing protocol like AODV[8], DSR[9] and OLSR[10] for wireless networks are not fitted for LLN due to its higher energy usage, repair in case of network failure and lack of consideration of node/link properties for establishment of routes[11], IETF ROLL working group

*E-mail address: bimalpatel.it@charusat.ac.in
ISSN: 1791-2377
doi:10.25103/jestr.141.03

comes up with RFC 6550 proposed standard RPL[6],[7] which is IPv6 based lightweight, distance vector, loop free, proactive source routing protocol applied for highly adaptive and dynamically changing network conditions with low power and lossy constraints personal area network. It fills the routing gap between LOWPAN and on other side IP world. RPL support mesh and hierarchical topology by considering routing through backup siblings/parent when needed based on the concept of "DODAG (Destination oriented directed acyclic graph)". Acyclic property helps to achieve loop free networks in a graph. RPL supports all three traffic types, i.e. P2MP (Point to Multipoint) in terms of downward routes, MP2P (Multipoint to Point) using upward routes towards LBR and P2P (point-to-point) for both transmission type like unicast and multicast.

1.1. RPL in Literature

It supports two route formation.MP2P traffic is supported using upward routes with the help of DIO and DIS messages for both grounded and floating node. P2MP and P2P traffic is supported using downward routes with the help of DAO message. It carries out both route formations with the help of neighbor discovery protocol which helps in local repair internally.

1.1.1. Upward Route

Grounded node acting as LBR or sink node broadcast DIO which contains necessary information like RPLInstanceID, Objective function(OF(0) or MRHOF)[12]–[14], version, trickle timer information and other parameters required for calculating rank to its neighbors[15]. If the node willing to join DODAG receive DIO message for the first time it adds its address to parent list and compute rank as per prescribed objective function and then multicast updated DIO message to others. If a node which is already part of DODAG receives DIO, it discards or process it by analyzing the mentioned criteria. Based on criteria if node's new rank is less than old rank, it changes its rank and updates its information to avoid loops else maintain its current position in DODAG. The journey of DIO propagation for forming an upward route is summarized in Fig. 2 using a flowchart.

1.1.2. Downward Route

P2MP and P2P traffic is supported by a downward route with the help of DAO control message. RPL uses two modes of operation for maintaining downward routes.1)Storing mode in which every router node maintains routing information2)Non-storing mode in which only sink node will have routing information and acts as source node to send traffic information to other nodes.

1.2. ROUTING ATTACKS AGAINST RPL NETWORKS

RPL routing protocol for 6LoWPAN due to its properties like limited processing power, changing network topology in terms of DODAG, link failures and mobility are prone to various network attacks. Broadly attacks can be classified as external attack affected by internet (example brute force attack and malware attack) and internal attacks due to wireless sensor networks. Again, internal attacks on overall network can be categorized as attacks targeting exhaustion of networks, attacks targeting RPL network topology and attacks against network traffic. In our work, we will focus on the sinkhole attack and in the further section, we will proposed trust based approach to detect and evaluate the various quality of service parameters[16]–[20].

1.2.1. Sinkhole Attack

In sinkhole attack malicious node by artificially changing rank somewhat higher than border router deceives legitimate nodes to get attacked towards itself claiming better path and link availability. As shown in below Figure 3 left-hand side shows a normal scenario where node 2 and 3 can be reached directly to sink node/border router but when node 6 advertise its rank lower artificially than nodes which are in the vicinity will get attracted towards it. All nodes 2, 3,5,7,9 and 10 will get attracted towards malicious node 6, which is shown in Figure 3. This attack is more devastating and cause larger network problems when it is combined with other attacks [16].

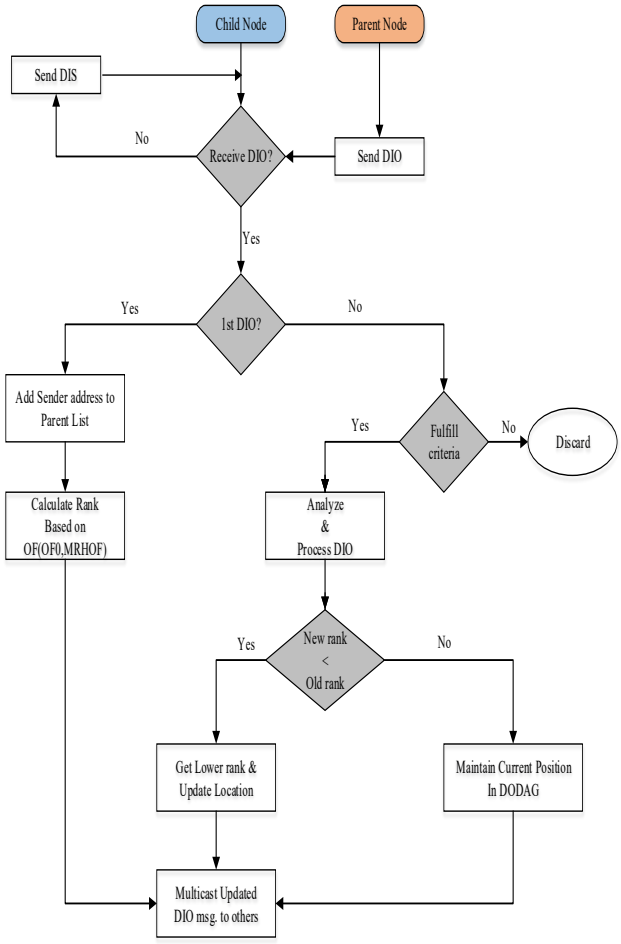

Fig. 2. Journey of DIO propagation

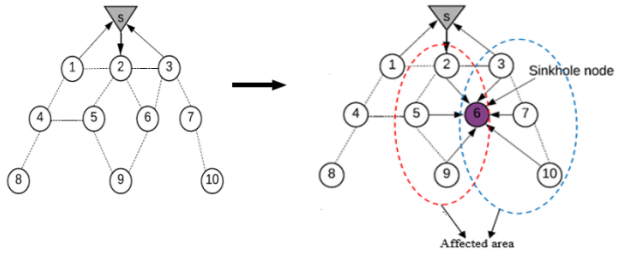

Fig. 3. Affected area after a sinkhole attack

2. Related Work

RPL due to its lossy nature and changing DODAG topology within 6LoWPAN are prone to external and internal attacks. Several recent literature studies have addressed the need for

detecting sinkhole and other attacks using IDS. The placement of IDS plays very important role in insider attack which disrupts routing service. Various studies have revealed that either placement will be distributed, centralized or hybrid. Detection method adopted by other related works are specification based, anomaly based or signature based[19], [20]. Sinkhole and Selective forwarding being a variation of denial of service attacks, whose role is to disrupt routing service and eventually degrade the quality of service parameters. In [17], [18] [21] author has suggested a hybrid approach called SVELTE combining signature and anomaly based detection for sinkhole and selective forwarding attacks. Due to mini firewall against global attack there was high resource consumption. The biggest drawback of scheme was it introduce high alarm rate, and even approach was considered only for small network size. In [22]–[24] author applied watchdog and trust based concept but has not considered the uncertainty factor. In selective forwarding attack (SF) the given techniques have high false positive and negative rate and approach doesn't perform well in mobility scenario. Due to low detection rate even PDR was less for SF, however it shows much improvement compared to the previous approach suggested by [svelte]. In [25] author evaluates compression header data of 6LoWPAN using machine learning algorithms called CHA-IDS, however this approach is only applied to a static network with limited in size. There are various other approaches related to machine learning [26] and fuzzy logic, but all introduce very low detection rate and high false alarm rate. In [27] author explored deep learning concept using machine learning techniques to negate denial of service attack. Using IRAD data set, three attacks are analyzed however it produce high false alarm rate. In [28] Fuzzy-IoT based two stage solutions is suggested, initially it provides much lower performance in terms of quality of service parameters but with time and larger network size performance improved. In the preceding section we will propose trust based detection approach, Direct Neighbor Sink reputed Trust based Intrusion Detection System (DSTIDS), considering uncertainty factor and calculating reputation at border router only to reduce overall overhead. Finally in result and discussion section our approach is compared further with Fuzzy-IoT and IRAD based on experimentation result considered from [29] along with actual concepts from [27], [28].

3. Proposed approach based on trust management

In this section, trust-based IDS is explored and proposed. A reputation system is a system where the behavior of a node are detected and evaluated by every node that is close enough to obtain a signal. These nodes examine the node and try to decide whether the node is behaving in compliance with the RPL protocol. There are many challenges to this, for example, because the malicious node is part of the reputation system, it may lie to the system and degrade its performance. Therefore, the system needs to be able to filter these messages. Another challenge is to minimal false positive and false negative rate. We proposed DSTIDS (Direct neighbor Sink reputed Trust based Intrusion Detection System) to secure RPL from routing attacks like a sinkhole and selective forwarding attacks.

3.1 Direct neighbor Sink reputed Trust based Intrusion Detection System (DSTIDS)

DSTIDS proposed model is based on two approach/stages. First, it records positive and negative observation at a specific node and based on particular observation opinion is considered using different trust values at sink/border router node. Based on the opinion, finally it is decided whether the node is malicious or not.

For a computational point of view, DSTIDS used different variable which are as follows:

– $Rd_{(BA)}$: Rank Deviation before an attack.
– $Rd_{(AA)}$: Rank Deviation after an attack.
– PR, NR and MNR: Parent Rank, Node Rank and Malicious node rank.
– PO, NO: Positive Observation and Negative Observation.
– W_{bel}: Weighing factor for belief.
– W_{disbel}: Weighing factor for disbelief.
– W_u: Weighing factor for uncertainty.
– t: is the time when trust is computed.
– W: The weight assigned to related individual parameter.

In the following theory, we explain several members of a model who are using the above variables that need further explanation. The overall flowchart for the proposed model is shown in below Figure 4.

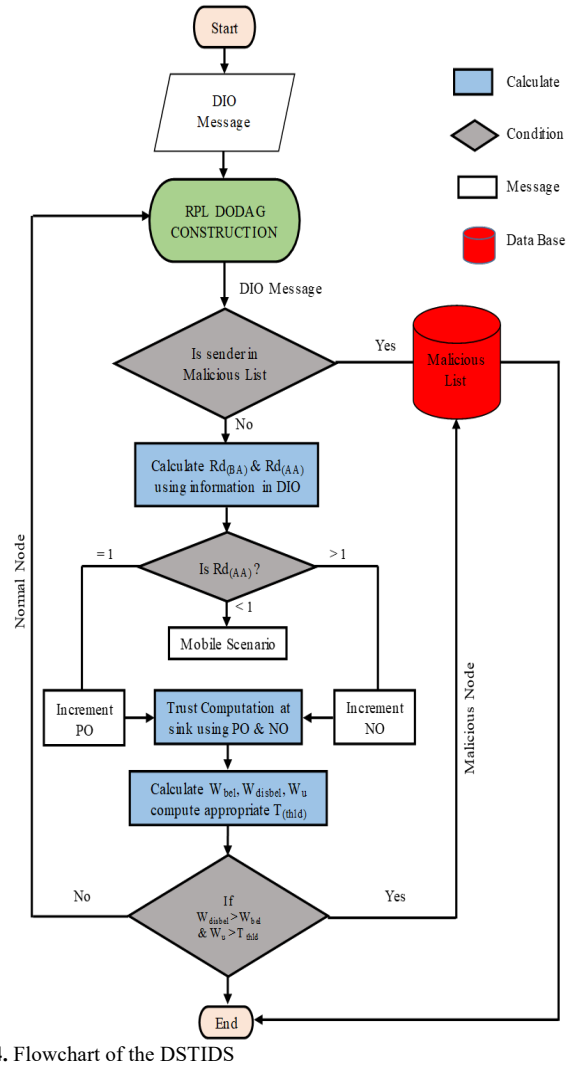

Fig. 4. Flowchart of the DSTIDS

3.1.1 Stage 1

After DODAG construction if any node behaves maliciously by changing rank or dropping data packets, DIO message received after an event or at specific fixed time interval (i.e. time update) is checked. Two variables that need to be checked are $Rd_{(BA)}$ and $Rd_{(AA)}$, Initially it is assumed that IoT network does not contain any malicious node when it is deployed, $Rd_{(BA)}$ is rank deviation before attack that will always remain 1 for OF (0) if attack is not involved in the system. As shown in Figure 3 left hand side if we calculate $Rd_{(BA)}$ based on Eq. (1) for node 10 it will be $|2-3|=1$. But if we calculate $Rd_{(AA)}$, which is rank deviation after attack it will have different values because malicious node infiltrates the network by declaring its rank to 1(greater than sink node). As shown in Figure 3 of right hand side after considering attack scenario if we now calculate the value of node 10 based on Eq. (2) it will be $|1-3| = 2$. So proposed approach considers DIO message to be malicious and increment the counter of negative observation by 1.

$$Rd_{(BA)}(n) = |PR - NR| \tag{1}$$

$$Rd_{(AA)}(n) = |MNR - NR| \tag{2}$$

$$Rd_{(AA)}(n) \begin{cases} > 1, NO = 1 \\ = 1, PO = 1 \\ < 1, Mobile \\ \quad Scenario \end{cases} \tag{3}$$

Based on values calculated by Eq. (2) for all nodes Eq. (3) will decide PO and NO and forward it to sink/border router. Overall Pseudo code for stage 1 is shown below in algorithm 1:

Algorithm 1

Pseudo code for node

Trust computing in a node
Malicious List = ∅
while *DIO received* **do**
  Initialize PO=0, NO=0
  if *Node from DIO* ∉ *Malicious List to* **then**
    Calculate $Rd_{(AA)}(n) = |MNR - NR|$
    if $Rd_{(AA)} > 1$
      NO++;
    else if $Rd_{(AA)} < 1$
      PO++;
    else
      //mobility scenario
    end if
  end if
end while

3.1.2 State 2

For the purpose of believing a statement we assume it will be either true or false. However, it is impossible to predict with certainty whether it is true or false so that we can only have an opinion about it. Trust between entities can be expressed using Subjective logic[30]. Based on opinion triangle trust values are referred as $W_{bel}(belief)$, $W_{disbel}(disbelief)$ and $W_u(uncertainity)$ [30], [31]. The values of these variables lie between 0 and 1 and their sum must be equal to 1, i.e. $W_{bel} + W_{disbel} + W_u = 1$. They are computed as

$$W_{bel} = \frac{PO}{PO+NO+K} \tag{4}$$

$$W_{disbel} = \frac{NO}{PO+NO+K} \tag{5}$$

$$W_u = \frac{K}{PO+NO+K} \tag{6}$$

The trust values are based on positive observation (PO) and negative observation (NO). A constant value k is used to simplify computations often it is set k=1 or k=2. A forgetting factor can be used so that more recent interactions get preference (i.e. higher weight) over older ones.

$$DSTIDS_{(ij)}(t) =$$

$$W_{bel} DSTIDS_{ij}^{belief}(t) + W_{disbel} DSTIDS_{ij}^{disbelief}(t) \quad \Rightarrow$$

$$+W_u DSTIDS_{ij}^{uncertainty}(t)$$

$$\Rightarrow W_{bel} + W_{disbel} + W_u = 1 \tag{7}$$

For example, Eq. (7) shows trust value evaluation using DSTIDS of node i for its neighbor j at time t, and takes values between 0 and 1. Eq. 8 shows an example of sink trust by border router for node j. Border router or sink node aggregates all values using subjective logic consensus operator ⊕. Be *v*1 = (*w*$_{bel}$*1, w*$_{disbel}$*1, w*$_u$*1)* the trust values of node i in node j and *v2 = (w*$_{bel}$*2, w*$_{disbel}$*2, w*$_u$*2)* the trust value of another node h in the same j. Then the combined trust of i and h in j is expressed by v1 ⊕ v2, which is defined below by Eq. (9)[31], [32].

$$DSTIDS_{(sj)}(t) = \frac{1}{n} \sum_{i=1}^{n} DSTIDS_{ij}\ (t) \tag{8}$$

$$\left(\frac{W_{bel}1\, W_u2 + W_{bel}2\, W_u1}{W_u1 + W_u2 - W_u1\, W_u2}, \frac{W_{disbel}1\, W_u2 + W_{disbel}2\, W_u1}{W_u1 + W_u2 - W_u1\, W_u2}, \frac{W_u1\, W_u2}{W_u1 + W_u2 - W_u1\, W_u2} \right) \tag{9}$$

$$DSTIDS^{Net}(t) = (W_{bel} + W_{disbel} + W_u)^{for\_all\_nodes} \tag{10}$$

$$if\ (W_{disbel} > W_{bel}\ \&\ W_u > T_{thld}) \tag{11}$$

Finally trust values of whole network $DSTIDS^{Net}(t)$ are calculated using Eq. 10, and with the help of Eq. 11 condition it is decided whether the node is malicious or not. If the node is malicious it is added to malicious list database, removed from the system and the decision is informed to other nodes of a system by border router. The only reason to calculate trust computation at a border router is to reduce the overall overhead of the system. Overall Pseudo code for stage 2 is shown in algorithm 2:

Algorithm 2

Pseudocode for border router and cluster head

Trust Computing at Border Router/Sink Node and Cluster-head (for mobile attacking node with small clusters)
if Periodic Trust packets with PO/NO are received from network nodes, cluster members **then**
  Calculate W_{bel}, W_{disbel} & W_u for every node
Combine trust values for every node to its reputation value
for DSTIDS $^{\text{for all nodes}}$ **do**
if ($W_{disbel} > W_{bel}$ & $W_u > T_{thld}$)
  Consider nodes as malicious
  Add to malicious list
end if
end for
  end if

4. Performance Evaluation

We have considered Contiki 3.0 [33] operating system running within an Ubuntu Linux virtual machine that has all the compilers, development tools, and simulators needed to this research Cooja, which is created by Adam Dunkels is flexible, extensible, discrete-event based and cross-level simulator included as a part of Instant Contiki which concentrate mainly on wireless sensor network behavior in IoT environment [24],[25]. This research implementation is based on Z1 nodes. We have considered 2 scenarios with varying % of malicious nodes and different network sizes to reach to an optimal result. In this simulation, the unit disk graph medium (UDGM) with distance loss radio model has been adopted as it provides a real-world emulation of the lossy links and shared media collision among IoT nodes. Since IoT nodes are lossy by nature, the reception ratio (RX) was set at a variable range of 70–100%. The overall configuration parameters for implementation purpose are given in Table 1 while specific parameters related to evaluation scenario is described in Table 2.

Table 1. Overall Configuration Parameters

Parameters	Values
OS	Contiki OS3.0
Mote Type	Z1 mote
Radio Medium	Unit Disk Graph
Model	Medium(UDGM): Distance Loss
DIO Min	12
DIO Doublings	8
RDC Chanel Check Rate	16
MAC Layer	IEEE 802.15.4
Duty Cycle	nullRDC
Network protocol	ContikiRPL
Objective Function	Hop Count of OF(0)
Attack Considered	Sinkhole Attack

Table 2. Parameter used for different Scenario

Evaluation Scenario	
Range of Nodes	Tx and Rx:50m,Interference :100 m
Tx/Rx Ratio	100/70-100
Size of Deployment area	100*100
No of Nodes	50,100,150,200,250
Sinkhole Rate	**Scenario#1:10%** | **Scenario#2:30%**
Time	30-45 min

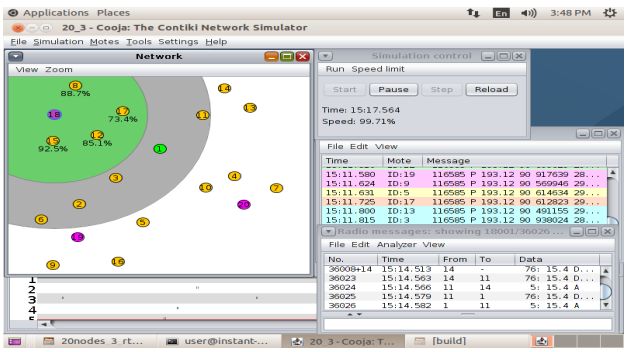

Fig. 5. Simulated view (Network Size 30 nodes, 3(10%) malicious nodes)

The simulated scenario with 10% malicious nodes for 30 network nodes is shown in Figure 5 for both sinkhole attack. Similarly 30% malicious nodes with 100 nodes as network size is shown in Figure 6 using Contiki 3.0 as operating system and Cooja as an incorporated simulator.

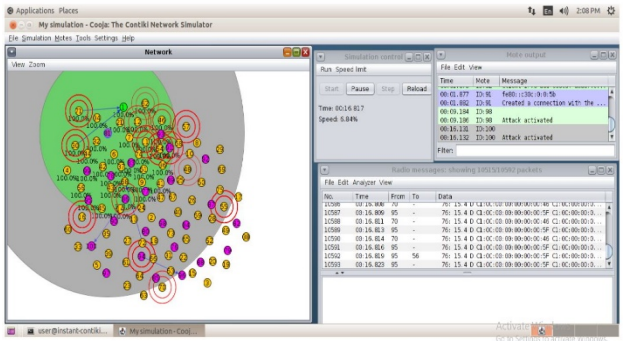

Fig. 6. Simulated view (Network Size 100 nodes, 30% malicious nodes)

4.1 Evaluation Metrics

To evaluate the performance of the proposed approach with standard RPL and RPL under sinkhole attack following quality of service measurement parameters are considered. Packet delivery ratio,Sensitivity rate/Detection rate and false positive rate are considered and evaluated[29], [36]–[39].

PDR: To evaluate routing effectiveness, packet delivery ratio is considered. It is the ratio of total packets received at destination (i.e. r_i) to the total number of packets sent by source (i.e. s_i). Eq. 12 illustrate formula to calculate PDR.

$$PDR = \frac{1}{n}\left(\frac{\sum_{i=1}^{n} r_i}{\sum_{i=1}^{n} s_i}\right) \times 100 \tag{12}$$

Detection Rate/TP_{rate}: It is the ratio of a number of attacker detected to the total number of attackers present.TP indicate true positive (i.e. normal node determined to be normal) while FN indicate false negative (i.e. malicious node is determined normal). Detection rate is calculated using Eq. 13 as follows:

$$TP_{rate} = \frac{TP}{TP+FN} \times 100 \tag{13}$$

FP_{rate}: It is the ratio of incorrect decision to all decision made for checking of normal nodes.TN indicate true negative (i.e. malicious nodes determined as malicious) while FP indicate false positive (i.e. normal node is determined malicious). Eq. 14 illustrate formula to calculate false positive rate.

$$FP_{rate} = \frac{FP}{FP+TN} \times 100 \tag{14}$$

4.2 Result and Discussion

We have considered a Contiki 3.0 operating system and cooja as a simulator to carry out various experiments. Firstly we will consider the quality of service parameters by considering standard RPL and RPL under sinkhole attack. For getting accurate values, the different proportion of malicious nodes and varying network size is considered. Figure 7 shows the packet delivery ratio (PDR) for sinkhole attack, due to sinkhole attack we get 60% to 85% delivery ratio compared to 95% to 99% in normal case. As shown in below figure if no of malicious nodes are about 30% and even there is an increase in network size there is drastic degradation of PDR compare to standard RPL.

Figure 8 shows optimal threshold values of false positive and false negative at which attacks are minimized. From figure it indicates optimal threshold values come out to be 0.65 for sinkhole attack.

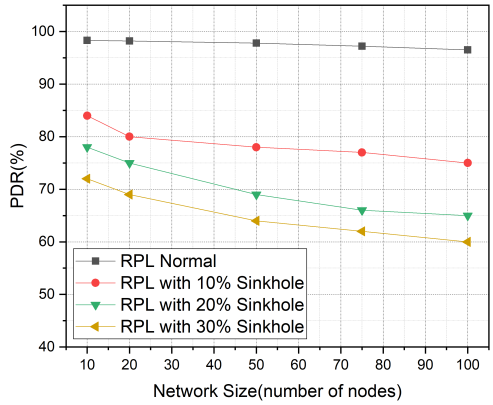

Fig. 7. Packet Delivery Ratio for Sinkhole Attack

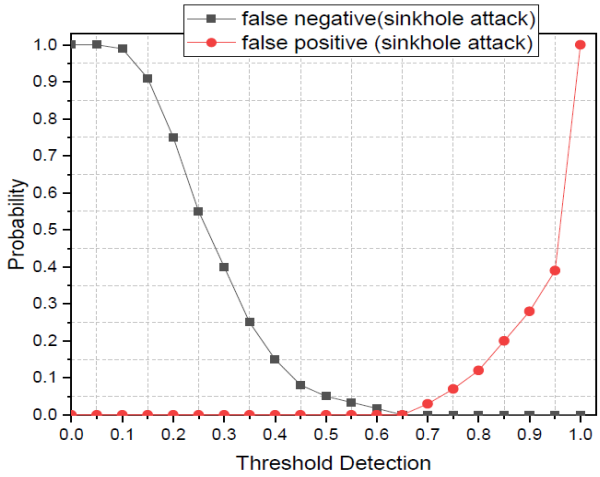

Fig. 8. False Positive and Negative threshold detection with different values

Performance and efficacy of proposed approach DSTIDS are compared with IRAD and Fuzzy-IoT. Comparison for related approach is considered based on experimentation carried out by [29] along with actual concept from[27], [28]. Two different scenarios (scenario 1:10% and scenario 2: 30% malicious nodes) is considered for sinkhole attack under varying network size.

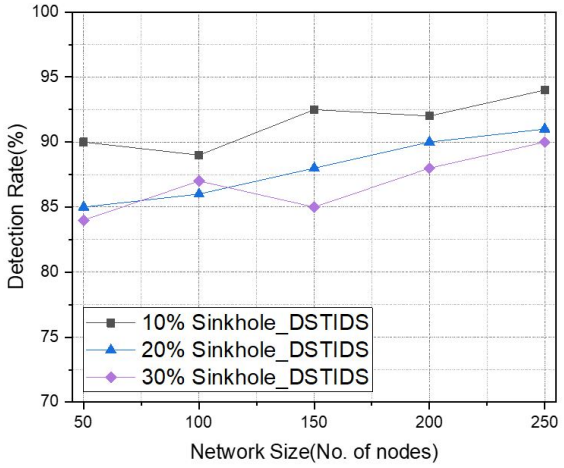

Fig. 9. Detection rate for sinkhole attack with different proportion of malicious nodes and network size

Figure 9 shows detection rate using DSTIDS for different scenarios under varying network size. For 10% sinkhole attack detection rate comes around 89 to 94% and for 30% it comes around 84 to 89%. As we can see from figure detection rate improves with increase in network size along with time.

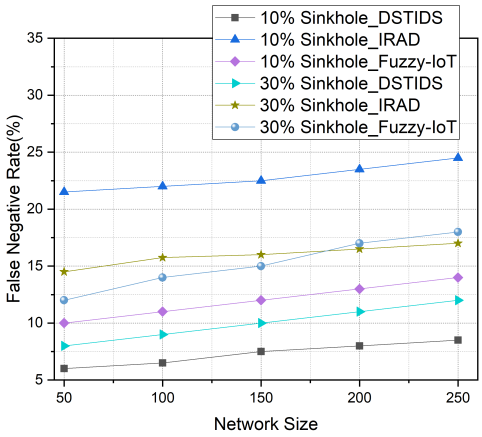

Fig. 10. FNR for sinkhole attack with different proportion of malicious nodes and network size

Figure 10 shows false negative rate (FNR) for all three approaches. Considering common example and IRAD as a base approach for comparison purpose, in case of 10% of malicious nodes with a network size of 100 nodes DSTIDS minify 70% and 20% FNR than IRAD and Fuzzy-IoT in terms of efficacy. Similarly for 30% malicious nodes, it reduces FNR up to 42% and 31% than IRAD and Fuzzy-IoT.

Figure 11 shows a false positive rate (FPR) for all three approaches. Considering common example and IRAD as a base approach for comparison purpose, in case of 10% of malicious nodes with a network size of 100 nodes DSTIDS minify 55% and 36% FPR than IRAD and Fuzzy-IoT in terms of efficacy. Similarly for 30% malicious nodes, it reduces FPR up to 54% and 13% than IRAD and Fuzzy-IoT.

Overall performance measurement in terms of FPR and FNR for direct neighbor sink reputed trust based intrusion detection system (DSTIDS) under two scenario i.e.10% and 30% sinkhole node with varying network size is shown in Table 3.

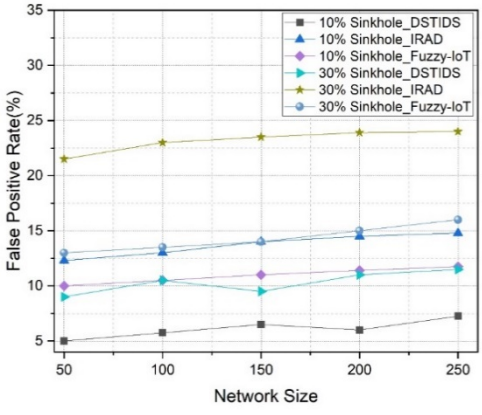

Fig. 11. FPR for sinkhole attack with different proportion of malicious nodes and network size

Table 3. Overall QoS performance measurement for DSTIDS

	Sinkhole (%)	Network Size	FPR	FNR
DSTIDS	10	50	5	6
		100	5.75	6.5
		150	6.5	7.5

		200	6	8
		250	7.25	8.5
	30	50	9	8
		100	10.5	9
		150	9.5	10
		200	11	11
		250	11.5	12

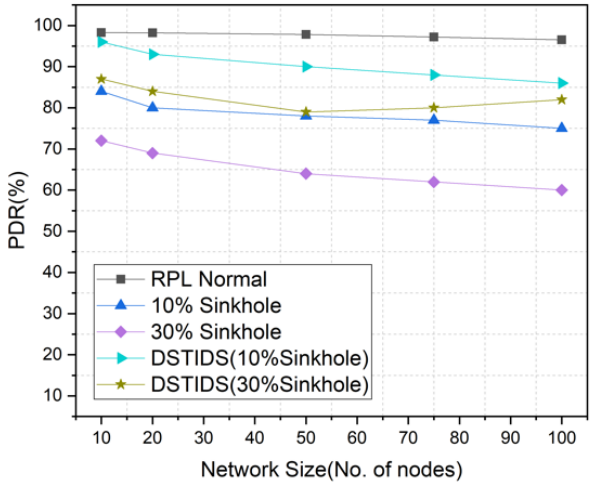

Fig.12. PDR using Standard RPL, Attack Scenario and Proposed Approach

Figure 12 shows the packet delivery ratio (PDR) after applying our proposed approach DSTIDS. The figure indicates that DSTIDS improve PDR roughly by 10 to 12% compare to attacking scenario of sinkhole attack for varying % of malicious nodes and varying network size. Summary of PDR values for DSTIDS is shown below in Table 4.

Table 4. Summary of PDR for DSTIDS

PDR	RPL Normal	10% Sinkhole	30% Sinkhole	DSTIDS_10%	DSTIDS_30%
10	98.3	85	72	96	87
20	98.2	81	69	92	84
50	97.8	78	64	90	79
75	97.2	77	62	88	80
100	96.5	75	60	86	82

5. Conclusion and Future Extension

As IoT environment is vulnerable to routing attacks due to heterogeneity in terms of smart things, constraint resources and complex infrastructure, an efficient trust based intrusion detection system called DSTIDS was proposed to mitigate the effect of a sinkhole attack in RPL for IoT deployment. To reduce overhead compare to other existing approaches trust calculation is considered only on border router along with consideration of threshold value and uncertainty factor. The proposed scheme is evaluated using Contiki 3.0 operating system with inbuilt support of cooja simulator and finally compared with other related approaches. Simulation results shows that DSTIDS provides better detection rate for varying % of sinkhole attack nodes and varying network size. Even our proposed scheme performs much better in terms of FPR and FNR compared to other existing approach. As a future work mobile scenario can be introduced along with a fixed network with the help of a mobility model and approach can also be evaluated and extended for other routing attacks like selective forwarding attack.

References

1. "Newsroom, Gartner, 2019." https://www.gartner.com/newsroom/id/2636073 (accessed Jan. 12, 2019).
2. L. Atzori, "The Internet of Things: A survey," *Comput. Netw.*, p. 19, 2010.
3. J. Gubbi, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, p. 16, 2013.
4. K. Lueth, "IoT market analysis: Sizing the opportunityKnud Lasse Lueth." Wiley, Accessed: Apr. 25, 2020. [Online]. Available: http://iot-analytics.com/wp/wp-content/uploads/2015/03/2015-March-Whitepaper-IoT-Market-analysis-Sizing-the-opportunity.pdf.
5. N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," *August 2007*, Accessed: Dec. 14, 2020. [Online]. Available: https://www.hjp.at/doc/rfc/rfc4919.html.
6. T. Winter *et al.*, "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," Mar. 2012, [Online]. Available: https://www.hjp.at/doc/rfc/rfc6550.html.
7. O. Gaddour and A. Koubâa, "RPL in a nutshell: A survey," *Comput. Netw.*, vol. 56, no. 14, pp. 3163–3178, Sep. 2012, doi: 10.1016/j.comnet.2012.06.016.
8. C. E. Perkins, M. Park, and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," p. 11.
9. D. Johnson, Y. Hu, and D. Maltz, "RFC 4728:The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Feb. 2007, [Online]. Available: https://www.hjp.at/doc/rfc/rfc4728.html.
10. T. Clausen *et al.*, "Optimized Link State Routing Protocol (OLSR)," p. 57.
11. P. Levis, A. Tawakoli, and S. Dawson-Haggerty, "Overview of Existing Routing Protocols for Low Power and Lossy Networks. draft-ietf-roll-protocols-survey-07." Apr. 2009, [Online]. Available: https://tools.ietf.org/html/draft-ietf-roll-protocols-survey-07.
12. P. Thumbert, "RFC 6552: Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)," Mar. 2012, Accessed: Dec. 14, 2020. [Online]. Available: https://www.hjp.at/doc/rfc/rfc6552.html.
13. P. Gnawali and P. Lewis, "RFC 6719: The Minimum Rank with Hysteresis Objective Function," Sep. 2012, Accessed: Dec. 14, 2020. [Online]. Available: https://www.hjp.at/doc/rfc/rfc6719.html.
14. J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "RFC 6551: Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks," pp. 1–30, Mar. 2012.
15. P. Levis, T. Clausen, J. Hui, and O. Gnawali, "The Trickle Algorithm(rfc 6206)," Mar. 2011, Accessed: Dec. 14, 2020. [Online]. Available: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Levis+P%2C+Clausen+T%2C+Hui+J%2C+Gnawali+O.+J.+Ko%2C%22+The+Trickle+Algorithm.+RFC+6206%2C+March%3B+2011.&btnG=.
16. B. Patel and P. Shah, "RPL routing protocol performance under sinkhole and selective forwarding attack: experimental and simulated evaluation," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 18, no. 4, p. 1849, Aug. 2020, doi: 10.12928/telkomnika.v18i4.15768.
17. A. Mayzaud, R. Badonnel, and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," p. 16, 2016.
18. A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion

detection system approach," *Int. J. Commun. Syst.*, vol. 25, no. 9, pp. 1189–1212, 2012, doi: https://doi.org/10.1002/dac.2356.
19. L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," *Int. J. Distrib. Sens. Netw.*, vol. 9, no. 8, p. 794326, Aug. 2013, doi: 10.1155/2013/794326.
20. A. Verma and V. Ranga, "Analysis of Routing Attacks on RPL based 6LoWPAN Networks," *Int. J. Grid Distrib. Comput.*, vol. 11, no. 8, pp. 43–56, Aug. 2018, doi: 10.14257/ijgdc.2018.11.8.05.
21. S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013, doi: 10.1016/j.adhoc.2013.04.014.
22. C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 606–611, doi: 10.1109/INM.2015.7140344.
23. M. Surendar and A. Umamakeswari, "InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar. 2016, pp. 1903–1908, doi: 10.1109/WiSPNET.2016.7566473.
24. A. L. Santos, C. A. V. Cervantes, M. Nogueira, and B. Kantarci, "Clustering and reliability-driven mitigation of routing attacks in massive IoT systems," *J. Internet Serv. Appl.*, vol. 10, no. 1, p. 18, Dec. 2019, doi: 10.1186/s13174-019-0117-8.
25. M. N. Napiah, M. Y. I. B. Idris, R. Ramli, and I. Ahmedy, "Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol," *IEEE Access*, vol. 6, pp. 16623–16638, 2018, doi: 10.1109/ACCESS.2018.2798626.
26. P. Bhatt and A. Morais, "HADS: Hybrid Anomaly Detection System for IoT Environments," in *2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, Dec. 2018, pp. 191–196, doi: 10.1109/IINTEC.2018.8695303.
27. F. Y. Yavuz, D. Ünal, and E. Gül, "Deep Learning for Detection of Routing Attacks in the Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, p. 39, 2018, doi: 10.2991/ijcis.2018.25905181.
28. M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)," *Computing*, vol. 101, no. 7, pp. 791–818, Jul. 2019, doi: 10.1007/s00607-018-0685-7.
29. M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism," *Wirel. Pers. Commun.*, vol. 114, no. 2, pp. 1287–1312, Sep. 2020, doi: 10.1007/s11277-020-07421-z.
30. A. Jøsang, "A LOGIC FOR UNCERTAIN PROBABILITIES," p. 33.
31. A. Jøsang and S. Knapskog, "A metric for trusted systems," NSA, 1998.
32. Z. A. Khan and P. Herrmann, "A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, Taipei, Taiwan, Mar. 2017, pp. 1169–1176, doi: 10.1109/AINA.2017.161.
33. A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in *29th Annual IEEE International Conference on Local Computer Networks*, Nov. 2004, pp. 455–462, doi: 10.1109/LCN.2004.38.
34. F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-Level Sensor Network Simulation with COOJA," in *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*, Nov. 2006, pp. 641–648, doi: 10.1109/LCN.2006.322172.
35. B. Patel and P. Shah, "Simulation, Modelling and Packet Sniffing facilities for IoT: A Systematic Analysis," *Int. J. Electr. Comput. Eng.*, vol. Volume 10, pp. 2755–2762, Jun. 2020, doi: 10.11591/ijece.v10i3.pp2755-2762.
36. J. Wang, S. Jiang, and A. O. Fapojuwo, "A Protocol Layer Trust-Based Intrusion Detection Scheme for Wireless Sensor Networks," *Sensors*, vol. 17, no. 6, Art. no. 6, Jun. 2017, doi: 10.3390/s17061227.
37. A. Le, J. Loo, K. K. Chai, and M. Aiash, "A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology," *Information*, vol. 7, no. 2, Art. no. 2, Jun. 2016, doi: 10.3390/info7020025.
38. F. Nygaard, "Intrusion Detection System In IoT," NTNU, 2017.
39. D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019, doi: 10.1016/j.future.2018.03.021.