This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.

InDReS: An Intrusion Detection and Response System for Internet of Things with 6LoWPAN

M.Surendar[1], A. Umamakeswari[2]
School of Computing, SASTRA University, Thanjavur, India
E-mail: [1]m.surendar@gmail.com,[2]a_umamakeswari@yahoo.com

***Abstract*—Internet of Things (IoT), an emerging Internet based technical architecture where heterogeneous sensors collaborate for ubiquitous computingbased on several technologies and standard communication protocols. With, such an amount of scaling and diverse technologies involved, IoT is susceptible to various threats. Hence, devising an IoT system,providing security through resistanceagainst attacks is a de facto requirement to make IoT secure and operational. The existing works for detecting adversaries like SVELTE and INTI consume too much resource. Further,packet dropping ratio is high and number of nodes taken for evaluation is low with some critical metrics overlooked. A novel detection technique with constraint based specification is proposed in this paper which significantly improves the shortcomings of SVELTE and INTI. The effectiveness of proposed scheme is valuated through comparative analysis using NS-2 simulation tool.**

***IndexTerms*—IoT, IDS, 6LoWPAN, WSN, INTI, RPL, Sinkhole, Specification IDS.**

I. Introduction

Intelligence in Things expresses a paradigm through which every object around us are connected through unique addressing, interact and cooperate to accomplish certain objectives irrespective of time and place [1]. The coordination of diverse technologies, heterogeneity and distributed nature of the network magnifies threats to IoT system. Furthermore, constraints such as limited storage, cost, power consumption, scalability and mobility, unique addressing of things has to be considered [2]. IPv6 over WPAN (Wireless Personal Area Network) referred to 6LoWPAN is a networking technology, that uses IPv6 protocol, enabling limitless scaling while retaining all the characteristics required for providing an unassailable IoT structure [3][4]. Wireless Sensor Network (WSN) is an integral part of IoT and can be subjected to various attacks with routing layer attacks being the most prominent one.

An Intrusion Detection System (IDS) examines activities in a network or node, detects attacks, alerts network and mitigatesthe harmful effect of the detected attacks. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), a routing protocol has inherent mechanism to defend against all severe attacks except sinkhole attacks even with DTLS, IPsec and IEEE 802.15.4 link-layer security applied [5][6]. There are slews of works for detecting sinkhole attacks on WSN [7][8]. Though, these are suited for WSN, they didn't consider IoT environment and few have postulated IDS for IoT with Shazid Raza et al. [6] comprehensive work being the initial attempt.

Subsequent works brought improvements over it, but still didn't provide the necessary Quality of Service (QoS) metrics.The IDS techniques are classified as Anomaly, Signature and Specification. Demerits of Anomaly are, it is resource hungry and have high false positives. Inability to detect unknown attacks disfavors signature method. Specification combines the merits of the other two methods and can be further sorted into constraint based and behavioral rule based. In this work, constraint based specification model is applied.

Our contribution constitutesproposing a novel effortat developing an Intrusion Detection and Response System (InDReS) which relies on constraint based specification model to detect sinkhole attack. We aspire to increase efficiency of QoS metrics andwhen attack is detected, malevolent nodes are isolated and network is reconstructed by isolating the malevolent nodes. Through simulation it can be seen that our proposed work is more efficient over existing INTI scheme on several QoS Metrics.

This paper is presented as follows: Section II portrays the related works. Section III specifies overview of research. Section IV describes the InDReS model and IDS algorithms. Section V presents Finite State Machine (FSM) model and Section VI the evaluation of InDReS through NS-2. Finally, Section VII presents the conclusion and future work.

II. Related Works

Literature worksfor intrusion detection system for detecting sinkhole attacks for IoT with 6LoWPAN, a protocol specifically designed for it are very less. IDS for Cyber Physical Systems, involves specific medical systemsand not recommended for typical IoT environment with many constraints [9]. Anhtuan Le et al.presented specification based IDS for RPL networks. Though, this can be considered as initial work, it could detect only two particular attacks and neither simulation results or numerical analysis were provided for validation[10]. SVELTEmethod detects attacks like sinkhole, selective forwarding and itemploys hybrid of both anomaly and specification based techniques. The drawback is high false positive rates and power consumption [6]. EBBITS [11], used Suricata, an open source IDS platform running on Linux host machine that can be regarded as network line of defense. It did not consider parameters associated with the nodes and focusses on host computer. INTI [12], used reputation and trust models for detecting sinkhole attacks. It reduced high false positives and improved mobility of SVELTE. But the limitation of both workis that somecritical QoS metrics were overlooked.

978-1-4673-9338-6/16/$31.00 ©2016 IEEE

III Overview of Research

A. 6LoWPAN

6LoWPAN, an open standard utilizes MAC and PHY layers of 802.15.4 standard, defines an efficient adaptation layer with IPv6 support with features such as routing, fragmentation, compression at network layer. It applies UDP at transport layer and messaging protocol like CoAP at application layer. End – to – End security is provided by DTLS. It's an IP layer based gateway allowing 6LoWPAN nodes to directly access internet[13].RPL, primarily used in a 6LoWPANnetwork, creates a destination-oriented directed acyclicgraph (DODAG) between the nodes in a 6LoWPAN. Each nodehas a rank and it decrease in the *up* direction towards theDODAG root and increase from the DODAG roottowards nodes. It supports both stateful and stateless modes.DODAGInformation Objects (DIO) are used to advertise information that are used to build the RPL DODAG.Every child node upon joining sends a Destination Advertisement Object (DAO). Parent nodes poll thesub-DODAG for DAO messages using DIO messages[14].

B. Evidence Theory

Compliance degree of a node is calculated based on Beta probability density function [9]. α and β are tunable parameters, determined based on the method of maximum likelihood by using the compliance degree history and evaluated using the constraint based specification technique.

Dempster-Shaffer evidence theory [15] [16], allows one to combine evidence from different sources and arrive at a degree of belief. An element in $P(\Theta)$ as a power set of system state Θ is called a system state hypothesis Hi, Θ → nonempty finite field. Through the observation results S1, S2, . . ., Sm for state by each sensor, DS theory can merge these results and infer the former state of system.

a) Basic probability assignment function (BPA) is defined as a map from a power set of Θ to [0, 1] interval. It is represented as $m : P(\Theta) \rightarrow [0, 1]$, $m(\Phi) = 0$,

$$\sum_{i=1}^{n} m(A_i) = 1, A_i \subseteq \Theta \qquad (1)$$

$m(A)$ → confidence value

b) Belief (Bel) measures the minimum or necessary support to the hypothesis, while Plausibility (Pls) measures the maximum or potential support.

$$\text{Pls (A)} = \sum_{B \cap A \neq \Phi} m(B) \qquad (2)$$

$$\text{Bel (A)} = \sum_{B \subseteq A} m(B) \qquad (3)$$

c) Dempster Combination Rules: Here A is a subset of Θ and coefficient $1/(1 - K)$ is usedas a normalization factor to prevent a nonzero value beingassigned to an empty set. The closer the value of K being to 1, the greater the confliction between the two evidences and vice versa.

$$m(A) = \begin{cases} 0, & A \neq \Phi \\ \dfrac{\sum A_i \cap B_j = A\, m_1(A_i) m_2(B_j)}{1 - K}, & A \neq \Phi, A_i, B_j \subseteq \Theta \end{cases} \qquad (4)$$

By combining values obtained through probability beta distribution and DS fusion rules, empirical value of 0.5 is assigned to the confidence level of node. Nodes above this value are considered good nodes and below as malevolent ones.

C. Research Motivation

In sinkhole attack an evil node attracts many nearby nodes to route traffic through it by advertising itself as trusted path to vital nodes. Failure to detect and address sinkhole will be catastrophic. There are many vital metrics like average energy consumption, packed drop ratio which are often not reckoned with IoT.In IoT environment, the lifetime of network is indirectly proportional to energy consumed. Moreover, the network response against any attack should be instantaneous since the sooner the network gets established the better for its reliable operation. There is a need to build a light weight model to identify the intruders at the earliest point in the IoT environment. Very limited works are available in the literature for IoT. This provided motivation to develop the detection mechanism.

IV InDReS Model

A) System Architecture

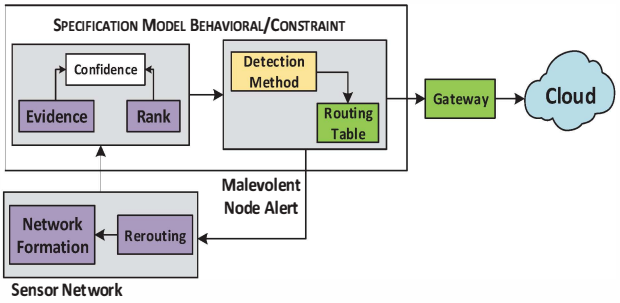

Fig. 1 InDReS Architecture

The functioning of InDReS architecture is explained in the following sections:

***Algorithm 1*: Leader Node Selection**

Let $SN_1, SN_2, \ldots\ldots SN_n$ be sensor nodes in the sensor network (n = total no. of nodes) and SN_{g1} sensor network group1 where g=1,2,3…m (m = no. of groups)
$P_i$be the probability of a sensor node SN_i, {i = 1,2…. n} to become L_{node}, ADV be the advertisement message and L_{node} be the Leader node.
Procedure L_{node}Sel()
For SN_i, i = 1 to n
{
If P_i = MAX
{

$SN_{i=} P_i$
Broadcast ADV $_{to}$ SN_{gl}
}
}

Algorithm Description: Each node elects itself as a L_{node}relying on a probabilistic strategy and broadcasts its availability to all the sensor nodes present in the group. Received signal strength, which is directly proportional to $P_{i.}$ determines $L_{node}$and distance between the nodes. The L_{node}does theaggregation of the packets received from all the nodes present in their group S_{g1}.

***Algorithm 2*: Calculating packet drop count**
Let P_{dc} be the packet drop count in the $SN_{g1.}$
Procedure Tup_{low}()
for SN_i= 1 to n
{
Calculate P_{dc}
return P_{dc}
}

Algorithm Description: The number of packets missed at the routing layer of 6LoWPAN are counted to determine how effectively the network handles the packets.

***Algorithm 3:*Malevolent node detection based on evidence**

Let SN_{ij}be the sensor node id, j represents the node id, SN_{ie}be the evidence value of nodes and TH_{val} be the threshold value for detecting evil nodes.
Procedureevidence ()
Assign TH_{val}
for S_{ij}, i = 1 to n
{
{
if SN_{ie}<TH_{val}
{
add malevolent node (S_{id})
goto rankdet();
}
}

Algorithm Description: The evidence value is calculated based on probability beta distribution function and DS theory is applied to each node on. If it is less than the threshold value, then the node is conceived as malevolent. Ranking algorithm is applied to affirm that it's an evil node.

***Algorithm 4:* Malevolent node detection based on ranking**
Let SN_{ir} symbolize the rank of nodes and SN_{ipr} be the rank of parent node. Initially malevolent node count is zero. Let malevolent node and its threshold be represented as M_{node} and M_{nodeTh}
Procedure ()
for SN_i, i = 1 to n
{
if
{
SN_{ipr}> SN_{ir} + R_{imh}
M_{node}++
}
}
for SN_i, i = 1 to n
if
{M_{node}>M_{nodeTh}
Alert network
}
}

Algorithm Description: Sum of rank of each node and minimum increase in rank from the current node to adjacent node is compared with the rank of parent node. If the summed up value is less than parent node, then the node is isolated and alert message is sent to the network and network topology is reconstructed.

V.FINITE STATE MACHINE MODEL

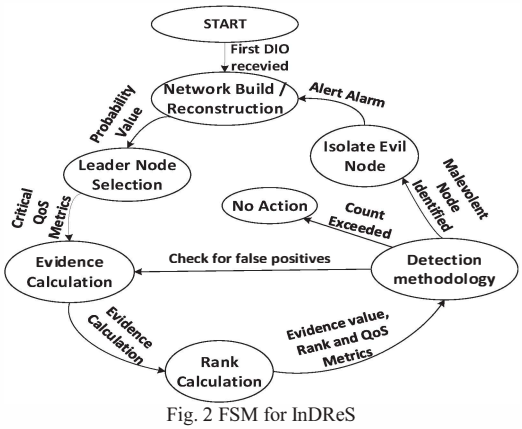

Fig. 2 FSM for InDReS

Sensor nodes are grouped into cluster and the maximum probability node becomes leader nodes and send announcement message to its adjacent nodes. Network is deployed with set of observer nodes. These nodes perform the node monitoring process and identifies the packet drop count of adjacent nodes. The observer nodes perform Dempster-Shafer estimation and apply ranking to each adjacent node. The output is compared with a threshold value to determine the malicious node. isolate and reconstruct the network.

VI.PERFORMANCE EVALUATION

Table 1 shows the simulation setup of the proposed model evaluated using NS-2.

TABLEI. SIMULATION SETUP

Sensor Nodes	150
Gateway	5
Base station	10
Transmission Range	100m
Initial Energy	100J
Observer nodes	30
Grid Size	500m X 500m

Hypothesis for the proposed work

a) All nodes are homogeneous
b) No Internet disconnection
c) Leader node can't be compromised

Performance of proposed scheme is evaluated in two scenarios. 1.Changing Node Density, 2. VaryingPacket Interval.Results for both settings are compared with existing scheme namely INTI.

Scenario 1: Changing Node Density

1. Packet Drop Ratio

The proposed scheme InDReSpacket drop ratio is less than INTI for all nodes as seen in Fig. 3. Packet Drop Ratio is the difference between number of packets sent and received.

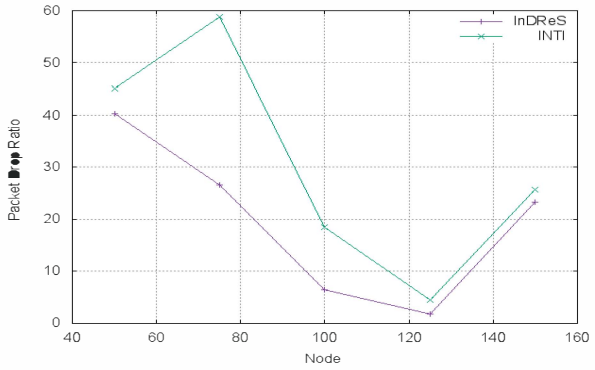

Fig. 3Packet Drop Ratio Comparison

2. Packet Delivery Ratio

InDReS achieveshigher packet delivery ratio than INTI and can be interpreted from Fig. 4. The ratio of received packets to packets sent gives the packet delivery ratio.

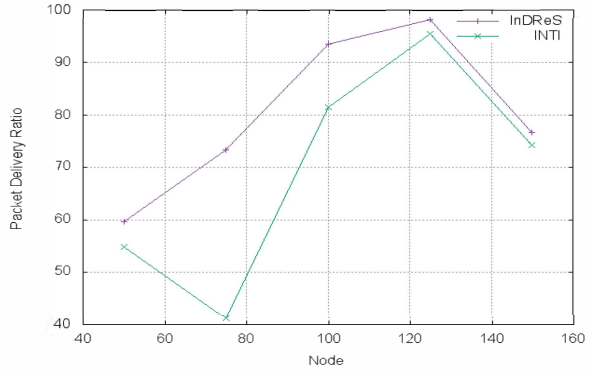

Fig.4 Packet Delivery RatioComparison

3. Normalized Overhead

The normalized overhead comparison is shown in Fig. 5

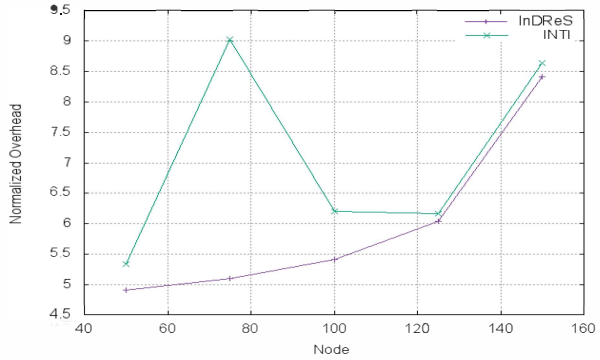

Fig.5Normalized Overhead Comparison

The normalized overhead is lesser in the proposed scheme. Normalized overhead is the ratio of control overhead to the received packets.

4. Throughput

Throughput is the number of successfully received packets in a unit time and it is represented in bps (bits per second). Proposed scheme has better throughput for all nodesas shown in Fig. 6.

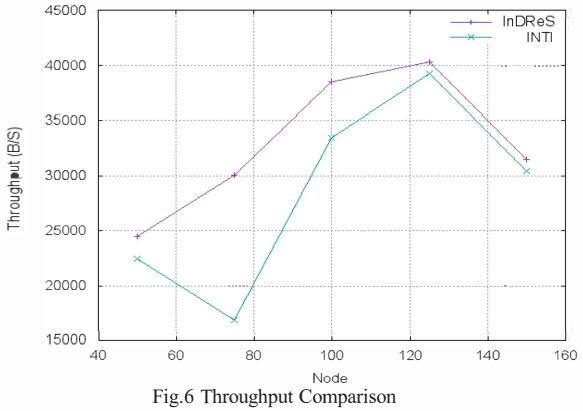

Fig.6 Throughput Comparison

Scenario2: Varying Packet Interval

1. Packet Delivery Ratio

InDReS accomplishes higher packet delivery ratio than the existing scheme with variable packet intervals and can be seen from Fig. 7.

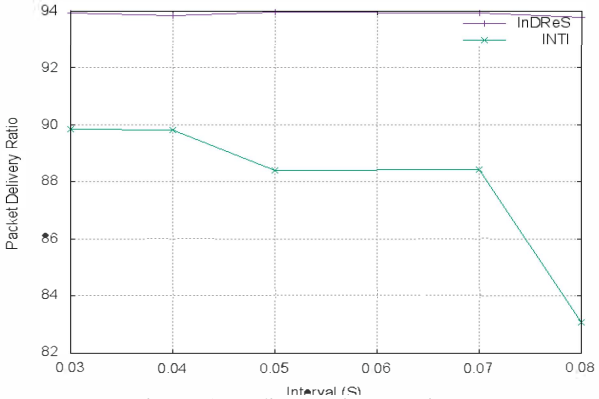

Fig.7 Packet Delivery Ratio Comparison

2. Packet Drop Ratio

The proposed scheme InDReS packet drop ratio is close to ideal condition for variable packet intervals as seen in Fig. 8.

3. Throughput

Throughput in our proposed scheme is better than INTI as seen in Fig. 9.

4. Normalized Overhead

Normalized overhead is less compared to INTI and shown in Fig. 10.

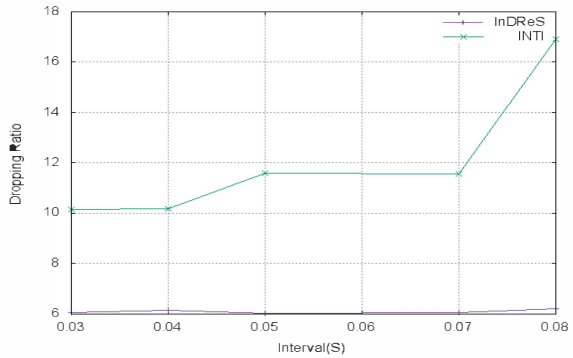

Fig. 8 Packet Drop Ratio Comparison

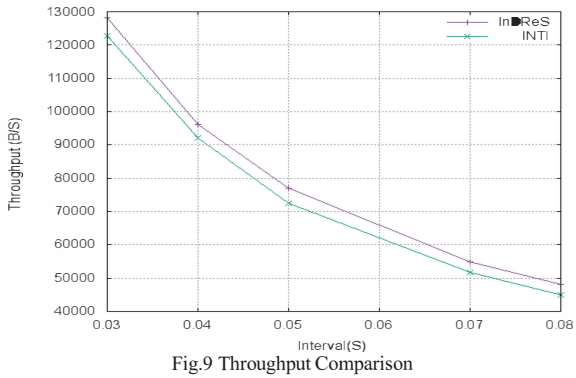

Fig.9 Throughput Comparison

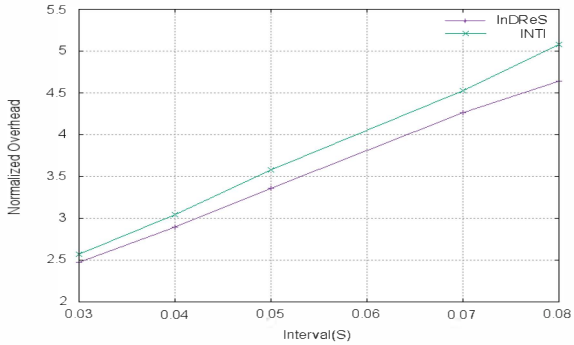

Fig.10 Normalized Overhead Comparison

5. Average Energy Consumption

Ratio of total energy consumed by all the nodes to the total number of nodes gives this metric as shown in Fig. 11.

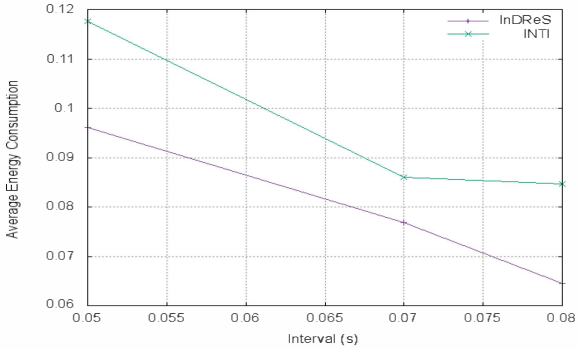

Fig.11Average Energy Comparison

VII. Conclusion and Future Work

The proposed work, InDReS is developed for resource constrained IoT network for detecting sinkhole attacks, using constrained based specification technique. This work has shown substantial improvement on many critical QoS metrics over the existing INTI scheme. As our future work, we intend to extend this work to use behavioral rule based specification with numerical analysis and utilize optimization techniques for RPL protocol.

Acknowledgment

The authors would like to acknowledge SASTRA University for the great support and assistance rendered to carry out this research work.

References

[1] Ovidiu Vermesan & Peter Friess, "Internet of Things – From Research and Innovation to Market Deployment," Revers Publishers,ISBN: 978-87-93102-94-1,2014.

[2] S. Sicariet al, "Security, privacy and trust in Internet of Things: The road ahead,"*Computer Networks*, vol.76, pp.146-164, 2014.

[3] Hanane Lamaazi et al, "Challenges of the Internet of Things: IPv6 and Network Management,"*Proceedings in the 8th International IEEE Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp 328-333,2014.

[4] Isam Ishaq et al, "IETF Standardization in the Field of the Internet of Things (IoT): A Survey,"*Journal of Sensor and Actuator Networks*, vol. 2, pp 235-287, 2013.

[5] Linus Walgren et al,"Routing Attacks and Countermeasures in the RPL-Based Internet of Things,"*International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-11, 2013.

[6] Shazid Raza et al, "SVELTE: Real-time intrusion detection in the Internet of Things,"*Adhoc Networks*, vol. 11, pp. 2661-2674, 2013.

[7] Robert Mitchell & Ing-Ray Chen, "A survey of intrusion detection in wireless network applications,"*Computer Communication*, vol. 42, pp. 1-23, 2014.

[8] Nabil Ali et al, "Intrusion Detection Systems in Wireless Sensor Networks: A Review,"*International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-7, 2013.

[9] Robert Mitchell and Ing-Ray Chen, "Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems,"*IEEE Transactions on Reliability*, vol. 62, pp. 199-210, 2013.

[10] Anhtuan Le et al, "Specification-based IDS for securing RPL from topology attacks,"*Proceedings in the International IEEE Conference on Wireless Days (WD)*,pp. 1-3, 2011.

[11] Prabhakaran et al, "Denial-of-Service detection in 6LoWPAN based Internet of Thing,"*Proceedings in the 9th International IEEE Conference on Wireless and Mobile Computing*, pp. 600-607, 2013.

[12] Christian Cervantes et al, "Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things,"*Proceedings in the IEEE mini-conference on International Symposium on Integrated Network Management*, pp. 606-611, 2015.

[13] N. Kushalnagar et al, "IPv6 over low-power wireless personal Area networks (6LoWPANs): overview, assumptions, problem statement, and goals,"*IETF, RFC* 4919, 2007.

[14] T. Winter et al, "RPL: IPv6 routing protocol for low-power and lossy networks,"*IETF, RFC* 6550, ISSN: 2070-1721,2012.

[15] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *Annals of Mathematical Statistics*, vol.38, no. 2, pp. 325–339, 1967.
[16] G. Shafer, "A Mathematical Theory of Evidence," Princeton University Press, ISBN: 0-608-02508-9, 1976.