A Multi-Attribute Trust-based Authentication Model for Internet of Things based Military Environment

B.Shadaksharappa, Prabhudeva V

Abstract: ***The Internet of Things (IoT) is an emerging field where physical objects are connected over the network, by the way, to make human life easy and more comfortable. The IoT environment is involved with various devices and those are working together to attain a common goal. The enhanced technology of IoT enables the military environment to work on it. Typically, most of the IoT devices are restricted in terms of their storage, process, compute and network capability. Hence, those devices are easy to attack and compromise. Compromised devices become behave as blackhole attacks. To assure the proper network function, we are in the situation to overcome those types of attacks. As trust plays a vital role in decision making, in this paper we proposed a Multi-attribute Trust-based Authentication mechanism (MTA). The ultimate aim of this model is to ensure authentication among the participating devices by identifying black hole nodes in the network. This multi-attribute trust calculation approach provides a maximum effort to evaluating the trustworthiness of devices. The simulation results show the applicability of the proposed model in terms of various performance metrics.***

Keyword: Internet of Things, Military, Security, Authentication, Trust and Blackhole.

I. INTRODUCTION

In the advancement of technology, the Internet of Things (IoT) is an emerging field that helps humans to lead their life in a better way. The recent surveys stated that the number of devices involved in IoT has been increasing tremendously and by the year 2025, 100 billion devices involved and will create a global economy about 11trillions USD (Rose et al, 2015). The concept of IoT is first proposed by Kevin Ashton in the year 1999 and he defined the IoT as uniquely identified things that are connected together with Radio Frequency Identification (RFI). (Shancang et al, 2015). Now the exact definition of IoT is given by various researchers and defined as collection of smart objects or things such as persons, devices, buildings, radio frequency identification tags, smart mobile phones, actuators, sensors, data resources and services, and any other smart devices that are connected together over an Internet by the way they can collaborate and communicate by sending and receiving data in order to attain a common goal by the way it helps human life become easy and more comfort.

Revised Manuscript Received on March 15, 2020.

Dr. B. Shadaksharappa, Professor (CSE) & Principal, Sri Sairam College of Engineering, Anekal, Bengaluru, Karnataka,India – 562106Affiliated to Visvesvaraya Technological University, Belagaum.
Email id: bichagal@yahoo.com; bichagal@sairamce.edu.in
Prabhudeva V, Enterprise Architect & Consultant, Tata Consultancy Services, Victor Building,ITPL, Bengaluru,Karnataka,India – 560066**.** Prabhudeva.vh@gmail.com;

The silent features of IoT provide a wide range of services in transport, community, national, home and etc. in transport services it is providing services in traffic and parking monitoring, logistics, emergency services, and highways management. In terms of home services, it offers entertainment, health, providing security and utilities and appliances.

In terms of community, it offers a monitoring environment, retail, factory, surveillance, business intelligence, and smart metering. Infrastructure, utilities, defense, remote monitoring, and smart grid these are the services are offering in national. In addition, industrialists, policymakers, doctors and caregivers, home/personal users and other individuals are using IoT (Jayavardhan et al, 2015).

At present, the need of IoT for the military is getting more attention because the modern military environment is a complex, dynamically changing environment, the commanders have less time in evaluating soldiers' decision during war and elaboration of operation plan, difficult in taking decision-based on collecting information (Bognar et al, 2018).

In the military environment, communications, computers, intelligence, controls, commands, surveillance and reconnaissance, personal digital assistants, cameras, handheld, and other devices are embedded with sensors to provide situational awareness to higher officials and warfighters on the ground, in the air and on the sea. (Denise at 2015).

The rest of the paper is organized as follows: Section 2 discusses the security issues in IoT based military environment. Section 3 discusses the need for trust in IoT based military environments. Section 4 discusses the related work. Section 5 discusses the proposed work, Results and discussion in section 6 and the final section concludes the paper.

II. SECURITY ISSUES IN IOT

Though IoT is offering a variety of applications, that unique characteristics such as the number of heterogeneous devices and networks, limitation in resources in terms of its memory, processing capabilities, computational capabilities, dynamic changing environment, and other limitations lead to security violations in the form of various attacks. (Abdelmuttlib Ibrahim Abdalla Ahmed et al, 2019). Security violations arise in various layers of IoT such as sensing layer, network layer, and application layers. In this work, we focus on the network layer. The main purpose of the network layer is routing the information among various communicating devices.

As the military deployed IoT, information that is sharing in this environment is always sensitive and more confidential. But protecting such information is always a critical task because security threats come in this form of various attacks such as spoofing, sinkhole attack, the man in the middle attack, eavesdropping, black hole and etc.(Bognar et al, 2018). Among the attacks, the black hole is considered as a more dangerous threat in compare with other attacks because it is launched from inside of the network by compromised nodes.

In this attack, a compromised device is broadcasting itself as they are having the shortest routes to the destination so that it is getting attention from other devices. Later, they are trying to drop the incoming packets which are intended to forward to other devices by it tries to save their energy. Since IoT entities are resource-constrained in nature, so the possibility of this attack is quite in common. (David et al, 2017) To ensure security among the communicating devices, the following security requirements are needed such as integrity, confidentiality, non-repudiation, authentication, and anonymity. Among the security requirements, authentication is important because it ensures the identity among the communicating devices in IoT based military environment. (Stankovic et al 2014). The authentication acts as a gateway for other security requirements hence once authentication is proved, other requirements can be easily achieved. It can be achieved in two ways one is pre-authentication and post-authentication. In this research work, we concentrate on the post-authentication mechanism.

Need of trust in IoT based military environment

Trust management is using in various fields of communication technologies such as Mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, bio-inspired networks and etc. The origin of trust is social trust and defined by "one entity is willing to depend on other entity" (Bamberger 2010). According to the network community, it is defined as a set of communications among the devices that contribute to the protocol which is built on earlier communication of devices within the protocol. (J S Baras et al, 2005, Liu z Joy et al, 2004) Trust management has the following properties such as context, subjective and objective. (Yan z, 2008, Yan z 2011, Yan Z 2014). Ensuring cooperation and collaboration among the participating devices is always a critical task.

Each device in the environment must trust other devices without prior recommendations and interactions such as blindness in communication will lead to security violations. However, to fulfil the assigned mission in IoT based military environment, every device is in the situation to ensure the identity of peer devices which is communicating that means authentication need to be provided. According to (Moyano, F, 2012). Trust models can be classified into two categories such as decision model and evaluation model. In this proposed model, we make use evaluation model in order to ensure the authentication of the participating devices. The trust evaluation is modelled based on the propagation, reputation, and behavior of the participating devices. In addition, to ensure the authentication various cryptographic methods are used such as digital signatures, key management, and various encryption and description algorithms. These methods are more effective but applying these algorithms for lightweight devices such as personal digital assistants, handheld devices, cameras, sensor-equipped monitoring devices, soldiers mounted packet radio and etc. will lead to security violations. The reason is the above algorithms always requires high processing, computational and memory capabilities.

Hence, applying those algorithms for these devices is impossible. To overcome the above shortcomings trust management comes into play.

RELATED WORKS

The following sections discuss the some of the existing work that related to the proposed work. The following section discusses some of the existing techniques that are available to ensure security in the IoT environment. Liang Liu et al, 2019 proposed the detection of multiple mix attack detection using both perceptron-based trust and K-means method. The proposed method is used to mitigate and detect three types of attacks such as tamper attack, drop attack and replay attack. Besides, to increase the detection accuracy further they have used an enhanced learning process. A mobile code-driven trust mechanism for detecting internal attacks is proposed by Noshina Tariq et al, 2019[28]. The main objective of the paper is to detect the black hole and grey hole attack by using the forwarding behavior of the sensor nodes.F.Ahmed et al, 2016 proposed a trust-based mechanism based on the forwarding behavior of the sensor nodes. The main objective of the paper is to detect black hole devices from the IoT environment. Chen et al, 2011 proposed fuzzy repudiation-based trust management to mitigate internal attacks. They have mainly considered the QoS metrics such as packet delivery, forwarding ratio, and energy consumption.

Bao F et al, 2013 proposed trust management based on direct and indirect recommendations. For both models, they make use of three trust properties such as honesty, the community of interest and cooperativeness. The main objective of the paper is to mitigate routing attacks. David et al, 2017 proposed a trust aware RPL routing protocol to detect black hole and selective forwarding attacks in the IoT environment.

In this model, the overall trust value is calculated only based on the forwarding behavior of the devices. Noshina Tariqa et.al, 2019 proposed a code driven based trust based model. The aim of this model is to isolate internal attack. Here the trust metric as only forwarding behaviour.

Proposed Model: Multi-attribute Trust-based Authentication (MTA) Assumptions and initial conditions

In this proposed model, we make use of the following assumptions and initial conditions. In this model, the terms things, objects, nodes, soldiers and entities are used interchangeably that are denoting the IoT components. The proposed MTA is designed irrespective of any routing protocol so it can piggyback with any routing protocol that suitable for the IoT environment. But in this proposed approach we make use of the Routing Protocol for Low power and Lossy networks (RPL) protocol as an underlying routing protocol.

In this mechanism, we concentrate on a post-authentication mechanism, therefore, MTA executed over the period when the performance of the network is likely degraded.

So, every node in the network executes MTA for identify untrusted nodes and excludes them by the way the authentication of each node in the network can be ensured. Initially, all the nodes in the network are trustworthy and well defined in terms of resources. Over the period they may change their behavior due to selfish or malicious.

To maintain the consistency of the network every node in the network must execute the MTA mechanism. Every node in the network maintains a table called Trust Table (TT) where aggregated trust information of nodes can be stored. All the aggregated trust values are in the range from 0 to 1. 0 represents minimum trust and 1 represents maximum trust. Every node is capable to calculate the trust values of others and not my own. Next, all the nodes in the mission are operating in promiscuous mode so it can overhear the forwarding behavior of their neighboring nodes. Assume the initial energy level of all soldiers 100%. The selfish or malicious nodes are represented as black hole attacks. The nature of the black hole attack is discussed in an earlier chapter.

Table 1. Structure of the TT table maintained by each node

TT table of nodei		
NID (j)	AT(j)	TUT

Where NID represents the evaluated nodes identity; AT represents the Aggregated Trust of neighboring nodes j and TUT represents the trust update time.

Multi-attribute Trust-based Authentication Model:

Over some time, performance of the network may degrade due to selfish or malicious nature of nodes so every node in the network must execute the MTA mechanism to identify untrusted nodes so that consistency of the network can be maintained. The proposed MTS consists of the following phases.

- Aggregated Trust Calculation
- Aggregated Trust Propagation
- Identifying untrusted nodes

Aggregated Trust Calculation

AT is calculated based on multi attributes such as direct, indirect, location awareness trusts of nodes, expected positive behaviour of nodes and energy level. As assumed all the nodes are in promiscuous mode, a node is capable to monitor and overhearing the forwarding behaviour of its neighbours. So, every node contains a list of their neighbouring nodes forwarding behaviours and as they are in the same communication range. According to the proposed MTA, every sender node i can receive passive acknowledgement from the immediate nodes as sender node places itself in promiscuous mode. Based on the passive acknowledgement received from the neighbour nodes, it will calculate direct, indirect trusts, expected positive behaviour and energy level. Location awareness trust can be calculated based on the frequency of its neighbouring soldiers.

AT values are calculated based on the fixed interval of time T. Over ΔT time every node had N number of interactions with their neighbouring nodes.

Direct trust calculation(DT)

Nodei evaluate direct trust of node j at time $t_i$based on two values such as number of successful packet forwarding ratio and reliability.It can be represented as,

$At\ time\ t_1,$

$$DT_{ij} = \omega_1 (p_{ij}) + \omega_2 (r_{ij}) \quad (1)$$

In the eq.1, DT_{ij} denotes direct trust of node j evaluated by node i, similarly,p_{ij} denotes the packet forwarding ratio (p) and r_{ij} denotes the reliability (r). Then,ω_1 and ω_2 denotes weighting factors and always $\omega 1+ \omega_2=1$, $i, j = 1,2,3$ ... and i ≠ j.

Packet forwarding ratio (p) is calculated from number of successful control and data packets forwarding from the overall forwarding ratio. The equation 2 depicts the packet forwarding ratio.

$$p_{ij} = \omega_1 (control\_packet_{ij}) + \omega_2 (data\_packet_{ij}) \quad (2)$$

Where$control_packet_{ij}$ denotes the control packet forwarding ratio of node j with respect to nodei and $data\_packet_{ij}$ denotes the data packet forwarding ratio of node j with respect to node i at timet_1.

Reliability is calculated by number of interactions between nodes. If the number of interactions between two nodes is high, reliability between the two nodes become high. It can be represented in equation 3.

$$if\ number\ of\ interaction > threshold\_1, R = 1$$
$$if\ number\ of\ interaction = threshold\_2, R = 0.5 \quad (3)$$
$$if\ number\ of\ interaction < threshold\_3, R = 0$$

Indirect trust calculation (IT)

Next the node i evaluates the indirect trust or recommendation trust of node j. To do that, node i send the request message for give recommendation about node j to its neighboring nodes k. Upon receiving the request message, the neighboring soldiers' also known recommenders k provides recommendations about node j to requesting node i. In that case, a greater number of recommendations leads extra computations for evaluating nodes. To avoid that problem, we follow the filtering mechanism. In that mechanism, we choose the recommenders k selectively based on threshold values. If the recommendation trusts greater than the threshold value, we take it into account. Otherwise discard them.

The indirect trust or recommendation trust is calculated by aggregation of direct trust of its evaluating node i and direct trust of recommenders k who had previous interactions with evaluated nodes j. The equation 4 denotes the indirect or recommendation trust.$At\ time\ t_1,$

$$IT_{ij} = \omega_1 (DT_{ij}) * \omega_2 (\sum DT_{kj}) \quad if \quad DT_{kj} > threshold\ value \quad (4)$$

$$otherwise\ 0.5$$

In the above equation 4, IT_{ij} denotes the indirect trust of node j evaluated by node i, DT_{ij} denotes direct trust of node j evaluated by node I, DT_{kj} denotes direct trust of node j evaluated by recommender

nodes k, Then, ω1 and ω2 denotes weighting factors and always ω1+ ω2=1, $i, j, k = 1,2,3$ ..., k≠ j and i ≠ j.

Expected Positive Behavior (EPB) calculation

Then node i calculate the Expected Positive Behavior (EPB) based on Beta distribution function. The purpose of beta distribution function is to model one's uncertainty about the probability of success of an experiment. For instance, over ΔT time node i may have n number of successful outcomes and n number of unsuccessful outcomes with node j. To predict the future behavior of node j, beta distribution function is used. Assume in a network, node i can have two outcomes, either success with probability p or failure with probability 1-p with node j. suppose also that p is unknown and all its promising values are considered equally likely. This uncertainty can be described by assigning top a uniform distribution on the interval [0, 1]. This is suitable since p being a probability can take only values between 0 and 1.

Besides, the uniform distribution assigns equal probability density to all points in the interval, which reflects the fact that no possible value of p is a priori deemed more likely than all the others. Now, suppose that node i perform n independent interactions of the experiment and observe p successes and p-1 failures with node j. After performing the interactions with node j, node i naturally want to know how revise the distribution initially assigned to p, to properly take into account the information provided by the observed outcomes.

In other words, node i calculate the conditional distribution of p, based on the number of successes and failures outcomes that node I observed. Consequently, the result of this calculation is a Beta distribution. The beta distribution function or beta random variable is described as follows,

$$P(x) = Beta(\alpha, \beta) = \int_0^1 u^{\alpha-1}(1-u)^{\beta-1}du \quad (5)$$

In the above equation, α and β are two indexed parameters, α>0 and β>0.

The expected value of beta random variable p is,

$$E(p) = \frac{\alpha}{(\alpha+\beta)} \quad (6)$$

In equation 6, α and β represents the good behavior and bad behavior respectively. Based on the equation 6nodeican calculate the Expected Positive Behavior (EPB) of node j by calculating number of successful transaction and unsuccessful transaction done by node j with respect to node I over Δt time.

The successful transaction is incremented by 1 for the evaluated node by the evaluating node if evaluated node j correctly forwarded the given packets. Otherwise its unsuccessful transaction is incremented by 1. It can be represented by,

At Over Δt time,

$$\alpha = s_{ij} + 1 \quad \text{and} \quad \beta = us_{ij} + 1 \quad (7)$$

From the equation 7, EPB of node j is calculated by substituting α and β values in equation 6. Therefore the following equation 8 represents the EPB of node j evaluated by node i.

$$EPB_{ij} = \frac{(s_{ij}+1)}{(s_{ij}+1)+(us_{ij}+1)} \quad (8)$$

In the above equation 8, EPB_{ij} represents expected positive behavior of node j evaluated by node j, s_{ij} denotes the successful transactions of node j with respect to node i,us_{ij} denotes unsuccessful transactions of node j with respect to node i, $i, j = 1,2,3$ ...etc.

Energy level calculation

After evaluating the EPB, node i calculate the energy level of node j. Every node in the network involved in network operations such as both control and data packet forwarding, receiving and overhearing. Consequently, their energy level will reduce and it ensures the lifetime of nodes therefore it consider as one of the factors in trust calculation. The energy level is calculated based on the equation 6.

At Over Δt time,

$$E_{ij} = IE_j - [\omega_1 \left[(N-1) * SENT_{Packets_j}\right] + \omega_2 \left[(N-1) * REC_{Packets_j}\right] + \omega_3 \left[(N-1) * OVR_{Packets_j}\right] \quad (9)$$

$$i, j = 1,2,3 \ldots N, i \neq j, \sum \beta_i = 1$$

In the above equation 9, E_{ij} represents the present energy of soldier j with respect to soldier i, IE_jrepresents the initial energy of soldier j, N represents the number of neighbor soldiers, $SENT_{Packets_j}$ represents the consumed energy while route discovery and route maintenance processes, $REC_{Packets_j}$ represents the consumed energy while route reply process and $OVR_{Packets_j}$represents consumed energy while monitoring neighbors behaviors. The percentage of present energy is calculated by equation 10.

$$\%E_{ij} = \left(\frac{E_{ij}}{IE_j}\right) * 100 \quad (10)$$

Based on the % of Energy (E), Energy Level (EL) is calculated and is classified into four categories that represented in the following table.

Table . Energy level

S.No	% of E	EL
1	>= 80	1
2	<80 &&>=50	0.8
3	<50 &&> 10	0.5
4	10<=	0

Location awareness Trust (LT)

Next node i will calculate the Location awareness Trust (LT) of node j. It reflects the stability of nodes in the network. But maintaining stability in such dynamic environment is a complicated task due to movement of nodes causes dynamic topology consequently variation in signal quality and loss. It affects the size, performance and state of the overall network. So it is necessary to know about the location awareness of nodes. It is measured by frequency in routing table entry of node j evaluated by node i. More entry of node j in the routing table of node i denotes higher stability in the presence of node i therefore location awareness trust of node' increases.

Otherwise decreases. The following equation 11 depicts the location awareness trust (LT_{ij}).

$$At\ Over\ \Delta t\ time,$$
$$\text{If frequency} > \text{threshold\_4}, LT_{ij} = 1$$
$$\text{If frequency} = \text{threshold}_5, LT_{ij} = 0.5 \quad (11)$$
$$\text{If frequency} < threshold\_6, LT_{ij} = 0$$

Aggregated Trust (AT) calculation

Before calculating aggregated trust, direct trust and indirect trust values are converted into composite values. Because those trust values are calculated at time t. Over the Δt time node i may evaluate n number of direct and indirect trust values of node j. On the other hand, factors such as expected positive behavior, energy level and location awareness trust are calculated over the Δt time. After the composite process, node i will evaluate the aggregated trust of node j based on the direct trust, indirect trust, expected positive behavior, energy level and location awareness trust based on the following equation 12.

$$AT_{ij} = \omega_1 (DT_{ij}) + \omega_2 (IT_{ij}) + \omega_3 (EPB_{ij}) + \omega_4 (EL_{ij}) + \omega_5 (LT_{ij}) \quad (12)$$

In the above equation, AT_{ij} denotes the aggregated trust of node j with respect to node i, $i, j = 1,2,3 \ldots N, i \neq j$ and $\omega_1 + \omega_{21} + \omega_3 + \omega_4 + \omega_5 = 1$.

Guarantee Authentication

Once aggregated trust is calculated, evaluating node i can decide on evaluated nodes j based on the threshold value. If aggregated trusts of node j satisfy the threshold value, they become trusted nodes. Otherwise they are untrusted nodes. Hence information about the untrusted nodes broadcast by evaluating nodes i. Therefore, entries of those nodes can be deleted from the trust and routing tables. By the way authentication of each node can be ensured.

Trust propagation and updating

Trust update process is carried out whenever the performance of the network goes down. Trust updating is achieved by trust propagation. Every node i after evaluating the aggregated trust of its neighboring node j, broadcast a special packet is called "Trust" packet where aggregated trust information are stored. After receiving the "Trust" packets, the neighboring nodes will update in the Trust Table (TT). In case, an old trust values are stored those values are replaced with new trust values.

Node's Dynamic Adaptation

Due to unstable environment of MANET, a node may join and may leave at any time in the network. Whenever these processes occur, dynamic adaptation algorithm is invoked. It described as follows; when a new node wants to join the network, first it will send the "NEW" request packet along with the aggregated trust of its own besides expiry time. Aggregated trust could receive by it in trust propagation phase. Based on the aggregated trust value possess by the new node, other nodes in the network make a decision on it based on the threshold value. If aggregated trust of new node satisfies the threshold value, it will participate. Otherwise it may discard by other nodes. Expiry time of new node denotes the waiting period to receive reply from others. If new node did not receive any response from others during the waiting period, it will reinitiate the NEW request packet. When a node wants to go off from the network, it will broadcast the leave packet therefore entry of that node deleted from the routing table as well as trust table.

Experimental results and discussion

The proposed model is implemented in Contiki/Cooja 3.0. The number of mobile nodes involved in the simulation is 75.

The total simulation run time is 600s. The movement of objects'/soldier's is restricted to a maximum of 2 m/s and used TMote Sky mote as mote type. The AT value of each node calculated at regular interval of 200s over 600s. Those nodes are placed randomly in 1000m x 1000m flat area. We have run the simulation three times for each interval. The maximum speed of mobile node is set to 20m/s and minimum is set to1 m/s. The node pause time is 0. The IEEE 802.11b is used as the medium access control protocol. UDP-CBR (Constant Bit Rate) is used as a traffic generator. The packet size is 64 byte with the data rate of 3072bps. The routing protocol used here is RPL. The selfish and malicious nodes are considered as black hole nodes. To analyze the impact of black hole node in the network, we have chosen randomly in increasing percentage. The proposed MTA mechanism is compared with standard RPL routing environment and (Noshina Tariqa et.al, 2019)

The proposed MTA consists of the following experiments

- Impact of black hole nodes over standard RPL routing protocol
- Detection ratio of black hole nodes under (Noshina Tariqa et.al, 2019) and MTA
- Performance metrics such as packet delivery ratio, throughput and end to end delay are compared with standard RPL and (Noshina Tariqa et.al, 2019)

Experiment1: Impact of black hole nodes under RPL routing protocol This MTA aims to ensure authentication by identify untrusted nodes means black hole nodes so it is necessary to know about the impact of black hole nodes over standard RPL routing protocol. To analyze, we increment the black hole nodes gradually and observed the impact. The following figure depicts the impact of black hole nodes. The figure1 shows whenever black hole node increases, packet dropping ratio is also increased gradually.

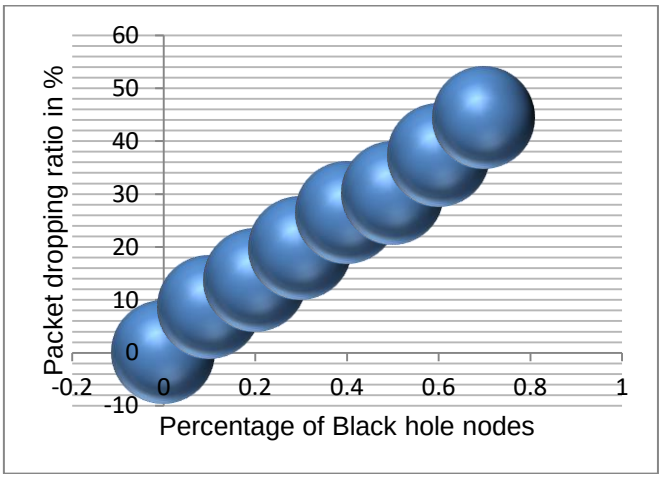

Figure 1: Impact of black hole nodes

Experiment 2: Detection ratio of Black hole nodes

In this experiment, we analyze the detection ratio of MTA over standard RPL and (Noshina Tariqa et.al, 2019).

Typically, RPL routing protocol is not having the ability of detection of malicious behavior in nature. Hence, we did not take into account. So here we analyze (Noshina Tariqa et.al, 2019) and proposed MTA.The following figure shows the detection ratio. It depicts detection ratio of MTA is gradually increasing compared with (Noshina Tariqa et.al, 2019). The reason is, in MTA we make use of multi attributes by the way we gave maximum effort to evaluate the trustworthiness of nodes. On the other hand, in (Noshina Tariqa et.al, 2019), only forwarding behavior as a primary metric to evaluate the trustworthiness. So, possibility of retain black hole nodes are still high. The packet detection ratio of MTA is 11.8% is high compared with (Noshina Tariqa et.al, 2019).

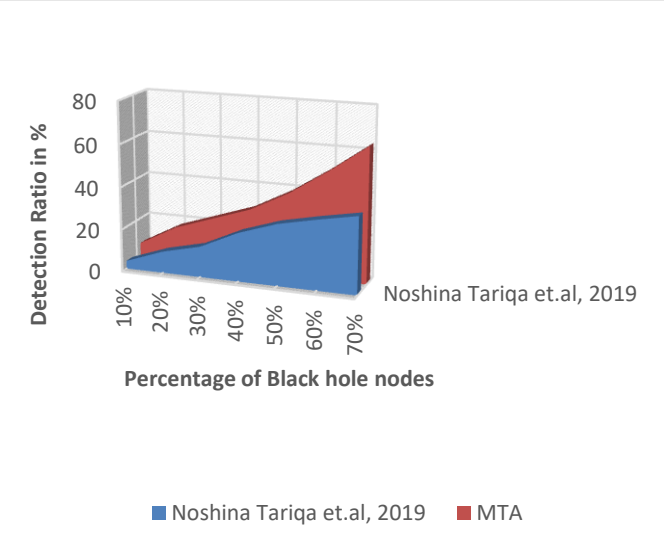

Figure: Detection ratio of black hole nodes under Noshina et al and MTA

Experiment 3: In this experiment, performance metrics such as packet delivery ratio, end to end delay, routing packet overhead and energy consumption are analyzed.

Packet delivery ratio

The following figure depicts packet delivery ratio of standard RPL, (Noshina Tariqa et.al, 2019) and proposed MTA. The figure clearly shows packet delivery ratio of MTA is high compared with RPL and (Noshina Tariqa et.al, 2019) even if percentage of black hole nodes is increased. The black hole nodes are identified and excluded from the network based on the AT values of MTA model before they involve in network operations therefore increasing packet delivery ratio. On the other hand standard RPL cannot detect black hole nodes naturally hence packet propped gradually when black hole node increases causes poor packet delivery ratio compare with Noshina Tariqa et.al, 2019and MTA. In (Noshina Tariqa et.al, 2019) due to weakest measurement of trust worthiness of nodes, probability of detecting black hole nodes is low consequently packet delivery ratio is also low compared with proposed MTA. From the simulation results we observed MTA provides 32.8% and 40.8% better packet delivery ratio compared with (Noshina Tariqa et.al, 2019) and standard RPL respectively.

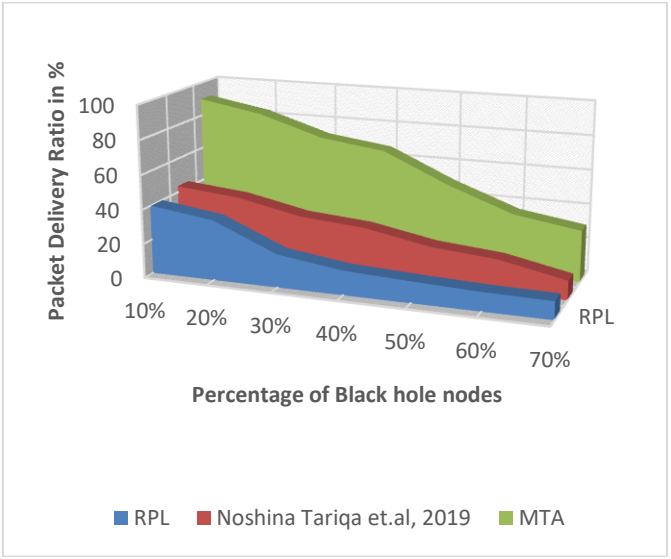

Figure. Packet Delivery ratio

Throughput:

The following figure depicts the throughput of MTA, (Noshina Tariqa et.al, 2019) and standard RPL. The figure depicts throughput of MTA is high compared with (Noshina Tariqa et.al, 2019) and RPL. The reason is misbehaving nodes are excluded after executing the MTA mechanism hence trusted nodes are participated in networking operations result is increasing throughput. In standard RPL, black hole nodes are affecting the nodes as lack of detection mechanism in RPL, packets are dropping increasingly consequently less throughput. Whereas in (Noshina Tariqa et.al, 2019) nodes are excluded only make use of forwarding behaviour metrics hence the probability of retain black hole nodes are high hence lower throughput compared with MTA. From the simulation results we observed MTA provides better throughput compared with RPL and (Noshina Tariqa et.al, 2019) about 21.7% and 24.1% respectively.

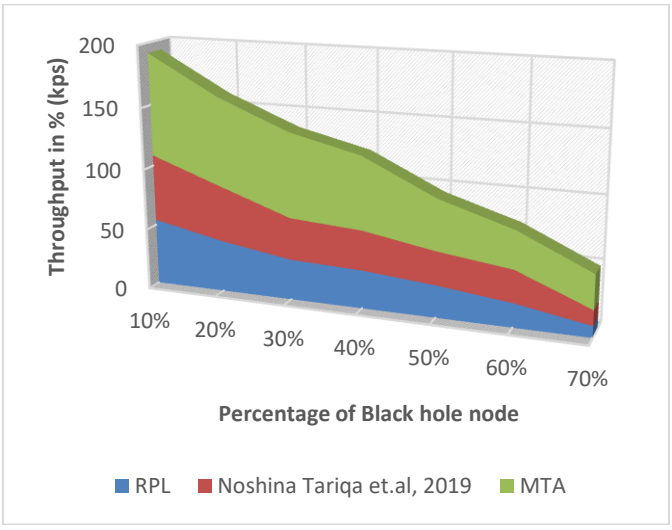

Figure: Throughput

5.8.3 End to end delay versus percentage of black hole nodes

The following figure 11 depicts the end to end delay versus the percentage of black hole nodes. The figure shows the end to end delay of RPL is high. As the presence of black hole nodes, packets are dropping constantly. Therefore, RPL requires retransmission of more packets and it leads to an increasing end to end delay. Both (Noshina Tariqa et.al, 2019) and MTA make use of trust concepts so they eliminated the misbehaving nodes from dropping the packets. However, when increasing misbehaving nodes, finding a trusted node in (Noshina Tariqa et.al, 2019) is difficult as the number of malicious nodes is increasing because it only focusses on a single attribute such as hop count. Whereas MTA gives maximum effort to identify untrusted nodes so the possibility of retransmission is relatively low compared with (Noshina Tariqa et.al, 2019). In the simulation, we observed that MTA is 18.8% and 12.5% decreased end to end delay compared with (Noshina Tariqa et.al, 2019) and MTA respectively.

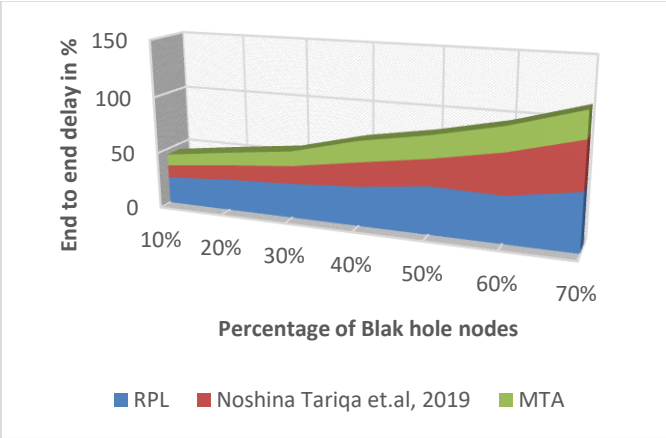

Figure .End to end delay

Table. Performance Comparison

		Routing Mechanism		
S.No	**Parameters**	**RPL**	**(Noshina Tariqa et.al, 2019)**	**MTA**
1	Packet delivery ratio in %	20.28571	28.28571	61.14286
2	Throughput in %	30.71429	33.14286	54.85714
3	Detection ratio in %	0	21.28571	33.08571
4	End to end delay in %	35.45714	22.94286	16.57143

III. CONCLUSION

In this work, we proposed a Multi- attribute Trust-based Authentication model to detect blackhole nodes in IoT based military environment. In this work, we are giving the maximum effort to evaluate the trustworthiness of the devices. Here, the aggregated trust is calculated based on direct, indirect, energy and location awareness trusts. The simulation results demonstrate that the proposed model is well compared with the traditional RPL routing and the existing model. The future direction of the work will concentrate on other security requirement such as confidentially and integrity.

REFERENCE

1. Rose, K., Eldridge, S., Chapin, L., 2015. The Internet of Things (IoT): an Overview–Understanding the Issues and Challenges of a More Connected World. Internet Society
2. Shancang Li & Li Da Xu & Shanshan Zhao, The internet of things: a surveyInf Syst Front (2015) 17:243–259).
3. Jayavardhana Gubbi,a Rajkumar Buyya,b* Slaven Marusic,aMarimuthuPalaniswamia) Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions.
4. BOGNÁR EszterKatalin,POSSIBILITIES AND SECURITY CHALLENGES OF USING IOT FOR MILITARY PURPOSES, Hadmérnök (XIII) 1II (2018) pp. 378-390.
5. (Denise E. Zheng William A. Carter, Leveraging the Internet of Things for a More Efficient and Effective Military, A Report of the CSIS Strategic Technologies Program, September 2015.)
6. Abdelmuttlib Ibrahim Abdalla Ahmed a,*, Siti Hafizah Ab Hamid b,**, Abdullah Gani a,***, Suleman khan c, Muhammad Khurram Khan d, Trust and eputation for Internet of Things: Fundamentals, taxonomy, and open research challenges, Journal of Network and Computer Applications 145 (2019) 102409)
7. David Airehrour Jairo Sayan Kumar and Ray Manukau 2017 A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks Australian Journal of Telecommunications and the Digital Economy 5 1.
8. Moyano, F.,Fernandez-Gago, C.,& Lopez, J.(2012,September). A conceptual framework for trust models. In Stankovic, J. A. (2014). Research directions for the Internet of things. IEEE Internet of Things Journal, 1(1), 3–9.
9. Bamberger and Walter 2010 Interpersonal Trust – Attempt of a Definition Scientific Report).
10. J S Baras and T Jiang 2005 Managing Trust in Self-Organized Mobile Ad Hoc Networks Proc. 12th Annual Network and Distributed System Security Symposium Workshop Liu z JoyA W and Thompson R A 2004 A Dynamic Trust model for mobile ad hoc networks Proceeding of the 10 th IEEE International Workshop on Future trends of distributes computing systems pp 80-85
11. Yan, Z., &Holtmanns, S. (2008). Trust modeling and management: from social trust to digital trust. IGI Global, 290-323.
12. Yan, Z., &Prehofer, C. (2011). Autonomic trust management for a component-based software system. IEEE Transactions on Dependable and Secure Computing, 8(6), 810-823.
13. Yan, Z., Zhang, P., &Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134.
14. Moyano, F., Fernandez-Gago, C., & Lopez, J. (2012, September). A conceptual framework for trust models. In International Conference on Trust, Privacy and Security in Digital Business (pp. 93-104). Springer, Berlin, Heidelberg.)