Open access Journal International Journal of Emerging Trends in Science and Technology
IC Value: 76.89 (Index Copernicus) Impact Factor: 4.219 DOI: https://dx.doi.org/10.18535/ijetst/v4i8.40

Ucon-Ipso: Usage Control with Improved Particle Swarm Optimization (Ipso) Based Hierarchical Security Framework for Attack Detection in Wireless Sensor Networks

N.Thangamani[1], S.John Grasias [2], Dr.G.Dalin[3]

Assistant professor [1], Assistant Professor& Head [2],
Department of Computer Science [1], Department of Computer Applications [2], AJK College of Arts and Science,Coimbatore-641 020, India.
[3]Asst Professor & Placement Officer PG & Research Dept of Computer Science Hindusthan College of Arts & Science,

ABSTRACT: In smart cities, Wireless Sensor Networks (WSNs) perform as a category of core transportation with the purpose of gathers information from the city in the direction of implement smart services. The security of WSNs is single of the key challenges of smart cities. Because WSNs are frequently organized in potentially difficult or still aggressive environment, an attacker is able to create each and every one type of threats and attacks. Many of the presented WSN security parts shouldn't consists of inconsistent attributes; consequently, conventional security parts shouldn't protect against ongoing attacks through dynamically changing attributes. To increase the security of WSNs, Usage Control with Improved Particle Swarm Optimization (IPSO) (UCON-IPSO) based security framework is proposed in this work which integrates attack detection and access control. Furthermore, different conventional prevention methods in WSNs, the proposed UCON-IPSO based framework make use of UCON with continuous decision making and dynamic attributes. These two attributes are useful in defending against ongoing threats. New UCON-IPSO security framework is proposed in the direction of protect Distributed Denial of Service (DDoS) and Sophisticated Attacks. The proposed UCON-IPSO based framework use a self-motivated adaptive likelihood discovery device and it also varied from conventional detection methods, which are able to revise dynamically toward protect against unknown attacks and DDoS attack. Lastly, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are used in the direction of execute attack mitigations when moreover low-level or high-level attacks are detected in this work. An experiment was performed in the direction of obtain an attack detection results for evaluation. The simulation results demonstrate the possibility and effectiveness of the proposed UCON-IPSO hierarchical security framework scheme with higher attack detection rate.

INDEX TERMS: Attack detection, Distributed Denial of Service (DDoS), hierarchical security framework, Improved Particle Swarm Optimization (IPSO), Network Function Virtualization (NFV), Software-Defined Networking (SDN), Sophisticated Attacks, Usage Control (UCON) and Wireless Sensor Networks (WSNs).

1. INTRODUCTION

A Wireless Sensor Network (WSN) is able to act as one category of core smart city communications [1]-[3]. Smart grids, smart transportation, smart government and rapidly be able to each and every one be recognized using WSNs. Moreover, the sensed information is able to also maintain extra smart city services. Consequently, the safety of WSNs is a key challenge for smart cities. Since WSNs are often organized in potentially difficult, an attacker is able to create each and every one type of threats and attacks [4]-[7]. Additionally in the direction of conventional threats, there is the option designed for highly developed continual threats, which are complicated ongoing and unknown attacks in WSNs [8-9]. Many of the WSN safety parts shouldn't consists of variable attributes; consequently, conventional security parts shouldn't protect aligned with ongoing attacks by means of dynamically changing attributes. As well, in usual Intrusion Detection Systems (IDSs) unknown attacks are observed as novel attacks since they forever includes novel properties, which varied from those of conventional attacks. Since many presented intrusion or attack prevention systems in WSNs are built with training data of known threats, they shouldn't protect against unknown attacks with the purpose of be able to cooperation the WSNs.

There are safety methods are previously used in many of the applications such as VoIP enterprise environments, trust administration, web services, and quickly with the purpose of were introduced to address several types of attacks such as ongoing and unknown attacks [10]-[13]. On the other hand, these schemes shouldn't be used straightforwardly in WSNs. Briefly, the advanced persistent threats created by ongoing and unknown attacks are able to break into WSNs and interrupt their normal tasks. Consequently, it is significant to propose an attack prevention scheme with the purpose of be able to improve security for WSNs .Presently there are two types of methods: detection-based approaches and prevention-based method to protect attack against WSNs is known as access control. Though several security schemes have been developed to solve intrusion detection and access control approaches for WSNs [1]-[5]. To increase the security of WSNs, a new security framework is introduced in this work which combines attack detection and access control.

In this work propose a Usage Control with Improved Particle Swarm Optimization (IPSO) (UCON-IPSO) based security framework to increase the security of WSNs at the same time as still taking the low-complexity and high safety of WSNs into account. The Distributed Denial of Service (DDoS) attack and Sophisticated Attack are detected by using UCON-IPSO security framework. Incoming traffic in the direction of the server is continuously monitored in the direction of directly identify any abnormal rise in the inbound traffic. This UCON-IPSO detection activates a rule with the purpose of pushes down the network traffic in the direction of a suitable level by discarding packets related to measured traffic levels of each of the dynamic sources. The attributes of continuous decision and dynamic attributes in UCON are able to deal with ongoing attacks by means of complex continual threat detection.

2. LITERATURE REVIEW

Krontiris et al [14] proposed a new rule based approach in the direction of detect sinkhole attack. They construct two rules and applied to Intrusion Detection System (IDS). When one of the rules is changed by one of the nodes, the IDs triggered an alarm on the other hand it couldn't give node ID of compromised node. The initial rule "for each overhead route modify packet the ID of the sender should be different your node ID". The second rule "for each overhead route modify packet the ID of the sender should be one of the nodes ID in the current neighbors".

Tumrongwittayapak and Varakulsiripunth [15] introduce a new Received Signal Strength Indicator (RSSI) value to Extra Monitor (EM) nodes to identify sinkhole attack. The EM have higher communication cost and one of their functions in the direction of compute RSSI of node and send to base station with ID of source and next hop. This process happens instantly when node are deployed. Base station makes use with the purpose of RSSI value in the direction of compute Visual Geographical Map (VGM). With the purpose of VGM shows the location of each node, then later when EM send updated RSSI value and base station recognize there is change in packet flow beginning earlier data this show there is sinkhole attack. The compromised node is recognized and isolated from the network through base station by means of VGM value.

Chen, et al [16], developed a new Girshick Rubin Shyriaev (GRSh) based algorithm designed for identifying the malicious nodes in WSN. Base station determines the variation of CPU usage of each node and identifies the present node is either malicious or not. Roy et al [17] presented a new trust management system to identify and eliminate multiple attacks. Each node computes the trust of its nearest node depending on the knowledge of interaction; reference and information then sends to base station. The base station determined which node is sinkhole subsequent to it established numerous trust values starting other nodes. Consequently the trust value of the node is higher than the 0.5 and is known as sinkhole attack [17].

Coppolino and Spagnuolo [18] proposed hybrid IDS to identify sinkhole attack and other attacks. This IDS use a detection agent to collect information of nodes and classifies the nodes are attacker or normal user. The hybrid IDS was attached to sensor node and share resource with the purpose of node. The suspicious nodes were inserted to the blacklist table supported abnormal behavior when analyzed the collected information from neighbors.Then that list is distributed to central agent to create decision depending on the feature of attack pattern

Papadimitriou et al [19] introduced a new cryptographic approach in routing protocol to detect sinkhole attack. Each node determines a public key which used in the direction of authenticate if the message comes from base station. They also used pair of public and private keys designed for validation and sign data message. Each and every one key were uploaded offline earlier than the network was deployed. These methods were prevented any node in the direction of conceal its ID and any packet forgery among nodes in the network. This protocol is focused on conflict in the direction of sinkhole attack however not to identify and eliminate it.

Fessant et al [20] proposed new two cryptographic protocols to increase the detection rate of sinkhole attack. These protocols prevent and detects malicious node from source to destination. On the other hand, they shouldn't show the memory usage of these protocols and message size. Disseminated beamforming clusters propose the possible to progress WSN energy effectiveness and decrease vulnerability in the direction of signal jamming attacks. On the other hand, they might be vulnerable in the direction of sybil attacks in which malicious nodes amplify their identities, consequently causing link failure appropriate in the direction of a smaller number of nodes participating in the collaborative transmission than predictable. Initially presents an analytic model in the direction of calculate the impact of these nodes, before integrating them into usual multihop reputation-based routing framework [21] with the purpose of adapts over time in the direction of use the nodes with the higher performance results. On the other hand, they may be susceptible in the direction of worm hole attacks in which malicious nodes amplify their identities.

3. PROPOSED METHODOLOGY

Usage Control with Improved Particle Swarm Optimization (IPSO) (UCON-IPSO) based security framework is proposed in this work which integrates attack detection and access control. Furthermore, different conventional prevention methods in WSNs, the proposed UCON-IPSO based framework make use of UCON with continuous decision making and dynamic attributes. These two attributes are useful in defending against ongoing threats. New UCON-IPSO security framework is proposed in the direction of protect Distributed Denial of Service (DDoS) and Sophisticated Attacks. The proposed UCON-IPSO based framework use a self-motivated adaptive likelihood discovery device and it also varied from conventional detection methods, which are able to revise dynamically toward protect against unknown attacks and DDoS attack. Lastly, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are used in the direction of execute attack mitigations when moreover low-level or high-level attacks are detected in this work. A simulation was performed in the direction of obtain an attacks for evaluation. This UCON-IPSO can address ongoing attacks using advanced persistent threat detection. Then, a NS2 network simulation tool is created in the direction of estimate the resource consumption and attack detection rate. The simulation results demonstrated that the proposed UCON-IPSO hierarchical security framework obtains higher efficiency and higher detection rate when compared to UCON framework. An experiment was performed in the direction of obtain an attack detection results for evaluation. In the proposed UCON-IPSO framework, rules are created to detect attacks. Since the resources of sensors are restricted however the sinks and base station contain higher computational resources and constant communication abilities to describes two levels of attack detection: (1) low level attack detection in sensors, and (2) high level attack detection in sinks and the base station

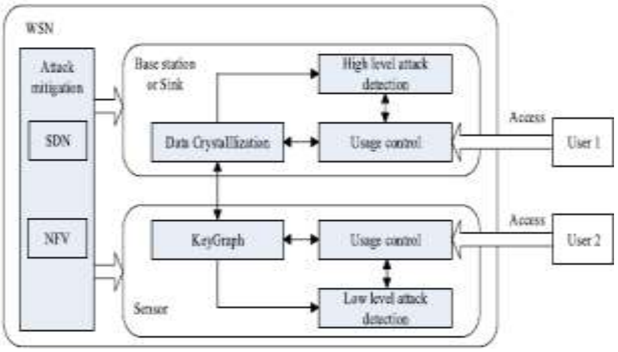

Figure 1. The proposed UCON-IPSO hierarchical security framework

High level attack identification methods needs comparatively difficult rules based on data crystallization and be able to change those rules continuously depending on the threat situation. On the contrary, the rules of low level attack identification using KeyGraph, it is easy algorithm and the rules are not changed continuously. A sensor will report unrecognized attributes in the direction of the sink if any unknown attacks or attacks occur at the sensor. Depending the high level rules, the sink node will then make a decision whether the events stop from an attacker or a normal user. The sink is able to modify the rules if essential related to the novel attack attributes and return a result if the attack shouldn’t be detected based on present rules. As well, attack mitigations designed for sensors, sinks and the base station are carryout depending on SDN and NFV.

3.3.1. REFERENCE MONITOR PROCESS OF UCON-IPSO

A Reference Monitor (RM) is one of the major important issues when applying UCON-IPSO for access control. ISO/IEC 10181-3 standard has been developed by the International Organization for Standardization (ISO) and provides a general security algorithm for RM access control.

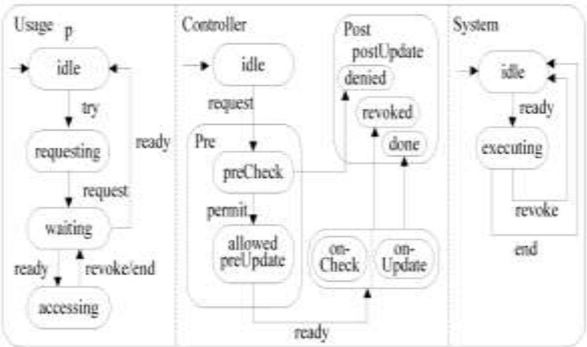

Figure 2. The core UCON-IPSO process

Though the standard documentation (ISO /IEC101181-3) designed for a tradition control procedure explains the system's fundamental behaviors, it requires structure. To increase the usage control system, UCON-IPSO is illustrated in state diagram is shown in Figure 2. UCON-IPSO usage control procedure is creating the try event basis a usages procedure p to be initiated in this work. At the establish any needed activities in the direction of start the usage procedure are performed in the request state. At the same time, the UCON-IPSO process creates the request event. Following the request event is named depending on the admission control policy; a preCheck state determination is beginning by means of the usage process p. Access control decisions are calculated with the purpose of point. When admission is denied, the controller begins some defined postUpdate actions. When admission is fixed, the controller launches every defined preUpdate action. Meanwhile, the ready event determination is created in this work.

3.3.2. KEYGRAPH BASED LOW LEVEL ATTACK DETECTION IN SENSORS

KeyGraph is used to extract the key points of the information and map the relations among them as an intuitionistic graph. The line among nodes in KeyGraph represents the relations between the information and quantifies the degree of tightness among the objects. KeyGraph is used to perform chance discovery. At initially, let us consider that the original data with set of access attributes S includes of a sequence of sets, represented by $s_1, s_2, \dots s_m, \dots s_n$, where each set s_m is a KeyGraph G$_m$. Related to the time complexity, an access time is splitted into n parts, and each access decision should be provided and chosen on time. The graph G$_m$ represents the access procedure from time t$_m$ to t$_{m+1}$, where each vertex of the graph is an attribute from node data of the access attributes, and each edge is a relation among two attributes. The iterations of chance discovery have been carryout as follows. Vertexes in G be able to be sorted related in the direction of the frequencies of the vertexes of the outer-edges in *Graph G*. The relationship of vertexes in G*, N$_i$ and N$_j$ in G* has been discussed as follows,

$$Connection(N_i, N_j) = \sum_{s_m \in D} |N_i, N_j|_{G_m} \qquad (1)$$

where N_i and N_j are vertexes of G_m and $|N_i, N_j|$ means the time gap of a directed line from N_i and N_j represented in graph model G_m, which related to the attribute set S_m. At this time, the relationship value be able to acts as an evaluation of the rigidity among N_i and N_j. Pairs of vertexes in G_i are described and sorted depending on the relationship among them, which is able to completely recognize the relationship and rigidity of a pair of vertexes. A line directed in the reverse direction should not be added into G_i since G_j is a directed graph. In KeyGraph, a connected sub-graph describes an entire procedure of rule creation, named a cluster. Related to the hierarchical formation of G_i for the base node, the layer is able to be calculated as the layer of its subnode. In G*,W(N, G*) is the value with the purpose of describes attribute N connected in the direction of the key links around it. The attribute nodes with values past a reasonable threshold are considered as detection rules with the purpose of should be assured for attack detection; therefore, a detection rule is able to be created.

3.3.3. DATA CRYSTALLIZATION BASED HIGH LEVEL ATTACK DETECTION

In the previous step KeyGraph is proposed for attack detection at lower level. In addition the KeyGraph model is extended to higher level attack detection by considering mahalanobis-distance. Let us consider that the θ feature matrix for attack detection and covariance matrix is denoted as H. Subsequently, depending on the computation of distance function is described in the following equation (2).

$$d_m = \sqrt{(\theta - \mu)^T . H^{-1} . (\theta - \mu)} \qquad (2)$$

where the lowest distance value is compared to threshold value of L_T , which is the distance from the usual recognized attack vertex in the direction of the usual access central vertex. Following adding together the virtual items, the KeyGraph be able to be reformulated. When the iteration is completed, the further added features must be confirmed by the recent attack dataset, which be able to optimize the KeyGraph. By means of this procedure, the virtual item determination is removed if it cannot equal the existing attack dataset. Lastly depending on the final KeyGraph, the results are able to be achieved and used for attack detection.

3.3.4. SECURITY ASSESSMENT BASED ON EVIDENCE

By Means of this procedure, an SDN controller gathers topology and susceptibility information instantaneously. The information majorly consists of network nodes, connectivity and vulnerabilities with the purpose of lie in the network nodes. It is simple for the SDN-MN controller because of its central authority role in the network. Subsequently, the SDN controller creates an attack graph by means of the present probabilities. Conventional NFV-based network defense machine identify real-time security events in the network and send them to the SDN controller. Then, the SDN controller calculates the present security level by using evidence-driven security assessment. Then new probabilities is created with the intention of be able to describe the present security level of the network. But this graph model is easily suffered from Denial of Service (DoS) attacks. So the higher level of the loss occurred from source to destination stage. So some new parameter is added to detect attack in this graph model. At the stage of attack graph measurement they need to calculate new value, assume that the $m_i(p_i; cost_i)$ be an attack mitigation control designed for action a_i and p_i denotes the probability of the success of a_i. At this time, $cost_i$ is denoted as the cost of attack mitigation mechanism. Then,

$$\Pr(a_j | m_j) = \Pr(a_j) \times p_i \qquad (3)$$

The major aim of this attack mitigation algorithm is to organize adequate attack mitigation controls so with the purpose of each and every one the probabilities of getting a target in the attack graph are below a specific threshold and at the same time, in the direction of hold the cost for deploying the attack detection controls in the direction of the lesser value in each and every one mitigation plans.

3.3.5. IPSO ALGORITHM FOR ATTACK DETECTION

This work presents a new intrusion detection mechanism for DDoS detection such as DAN, which classified into the Network Traffic Analyzer, Traffic Features Identification and Extraction, and Intruder Information. IPSO uses a number of particles and it is considered as the nodes in the graph model, which represent a swarm moving around in the search space, in the direction of look for attack detection. Each particle is considered as an attack detection point in a D-dimensional search space in the graph model, which adjusts it's "flying" related to its own flying knowledge and compared them to the other particles. The particles flight by means of a specific velocity in the D- graph model to find the optimal attack detection. The velocity of node(Patricle) i expresses as V_i= (v_{i1}, v_{i2}, ..., v_{iD}), the position of node (particle i) is denoted as (x_{i1}, x_{i2}, ..., x_{iD}), the optimal detection results of the attacks is denoted as P_i= (p_{i1}, p_{i2}, ..., p_{iD}), it is also called pbest. The global optimal results of attack detection results for all nodes in the network model is represented as P_g= (pg_1,pg_2, ..., pg_D), it is also named as gbest. Each node in network graph model has a fitness function (Cost(T)) to determine the fitness value. In general PSO algorithm, the velocity update formula to d-dimensional graph search space in formulae (4) and (5):

$$\mathrm{v_{id}} = \mathrm{w} \times \mathrm{v_{id}} + \mathrm{c_1} \times \mathrm{rand(\quad)} \times (\mathrm{p_{id}} - \mathrm{x_{id}}) + \mathrm{c_2} \times \mathrm{rand(\quad)} \times (\mathrm{p_{Gd}} - \mathrm{x_{id}}) \qquad (4)$$

$$x_{id} = x_{id} + v_{id} \qquad (5)$$

Where , Q is denoted as the population quantity, w is denoted as the inertia weight, $C_1$and C_2 represents the acceleration constants it is equal to 2 [22], v_{max} denotes the maximum velocity of the particle, G_{max} represents the maximum number of iterations, rand ( ) and Rand ( ) are random functions with values in [0,1].

Improve inertia weight : Inertia weight is a major factor of the conventional PSO algorithm. It computes the final results of PSO. Fixed inertia weight always reduces the results. Formula (6) is the velocity formula with a predefined inertia weight in conventional PSO algorithm [22]:

$$v_{id}(t+1) = w \times v_{id}(t) + c_1 \times rand(\quad) \times \left(p_{id} \times x_{id}(t)\right) + c_2 \times rand(\quad) \times \left(p_{gd} - x_{id}(t)\right) \qquad (6)$$

Related to concept , w normally takes between 0 and 1[22]. Consequently, w is 0.9 in this work. The velocity formula (5.5) is changed into formula (5.6):

$$v_{id} = 0.9 \times v_{id} + 2 \times rand(\quad) \times (p_{id} - x_{id}) + 2 \times rand(\quad) \times \left(p_{gd} - x_{id}\right) \qquad (7)$$

Presently, the traditional strategy of increasing inertia weight is Liner Decreasing Inertia Weight (LDIW). The modified way of inertia weight w described in formula (5.7):

$$v_{id} = w \times v_{id} + 2 \times rand(\quad) \times (p_{id} - x_{id}) + 2 \times rand(\quad) \times \left(p_{gd} - x_{id}\right) \qquad (8\ )$$

$$w = \begin{cases} w_{end} + (w_{start} - w_{end})\left(1 - \dfrac{T}{G_{max}}\right) \ if\ p_g \\ w_{end}\ if\ p_{gd} = x_{id} \end{cases} \qquad (9\ )$$

where T is the total number of iterations, $T \in [0, G_{max})$, p_{gd} is denoted as the global optima results for attack detection, w_{start} is denoted as the initial inertia weight value and w_{end} is denoted as the final inertia weight value in the maximum iterations are calculated simultaneously. In order to solve speed of PSO algorithm, the constriction factor is introduced in this work is showed in formula (5.10):

$$K = \frac{\left(\cos\left(\frac{\pi}{G_{max}}\right) \times T\right) + 2.5}{4} \qquad (10)$$

where T is the maximum number of iterations. Set G_{max}= 40, the changing curve of value K shows in Figure 3.

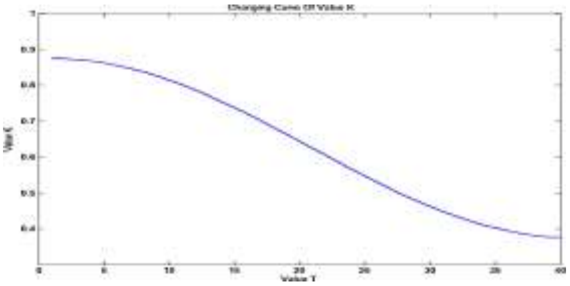

Figure 3. The changing curve of value K

The curve of K in the Figure 3 is denoted as the objective function or cost function. The value K is substituted informula (5) turns into formula (11). Formula (11) is denoted as follows,

$$v_{id} = \frac{\left(\cos\left(\frac{\pi}{G_{max}}\right) \times T\right)}{4} \times \left[v_{id} + 2 \times rand(\quad) \times (p_{id} - x_{id}) + 2 \times Rand(\quad) \times (p_{gd} - x_{id})\right] \qquad (11)$$

The PSO algorithm with constriction factor is special type of the PSO with new modified inertia weight and it is able to increase the speed of the algorithm. Constriction factor K increase the speed of PSO and inertia weight influence the degree of maintaining the new velocity. Depending on the different constriction factor and inertia weight, then determined optimal path P$_i$(T). Let M = {m$_i$|, i=1,…N$_a$} be the attack mitigation controls for the actions A = {a$_i$|, i=1,…N$_a$}. A Boolean vector T = {t$_i$|, i=1,… N$_a$ } is used to present the attack mitigation plan, where t$_i$ True means that m$_i$ is adopted in the plan, and t$_i$ ∈ False means that m$_i$is not adopted in the plan. Let us consider that there are p number of paths in the attack graph, and T is the attack mitigation plan. The maximum value in the attack mitigation model is Threshold. Subsequently, the probability of a successful attack for the ith path is P$_i$(T), and the total cost of attack model T is denoted as Cost(T). In the direction of reach the aim of an attack mitigation model, the values should conform the policy.

$$\mathrm{P_i(T) \leq Thershold, i = 1,..p} \qquad (12)$$

This is similar to

$$G_i(T) = P_i(T) - Thershold \leq 0, i = 1,..p \qquad (13)$$

In WSNs, the sink and base node generally have powerful resources; however resources at the sensors are restricted. Consequently, the resource consumption of the proposed UCON-IPSO scheme (time and memory) in sensors is very significant. To perform the evaluation, proposed UCON-IPSO scheme was implemented based on TinyOS.

4. SIMULATION RESULTS

To achieve the data set designed for evaluation, an attack detection simulation was performed. The WSNs are connected through Wi-Fi for the experiment since several existing real-world WSNs make use of Wi-Fi technologies. In the initial stage of the work node initialization and creation is formed by using MATLAB tool is illustrated in figure 4.

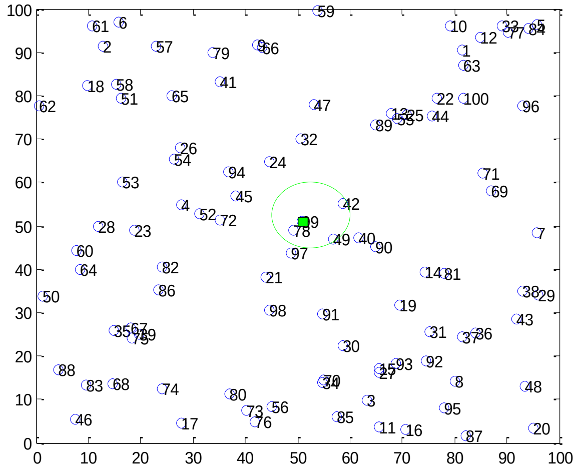

Figure 4. Network formation

The shortest distance path among different sources to destination is shown in Figure 5 for UCON.

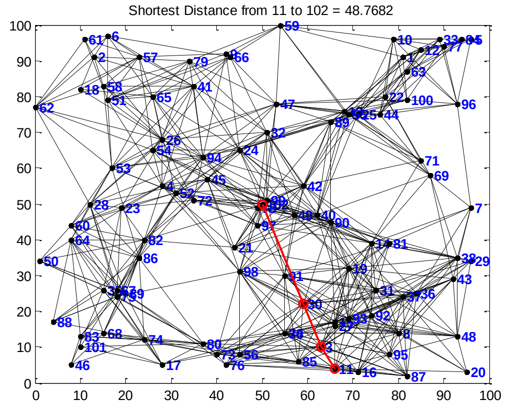

Figure 5. Shortest distance path from path 11 to 102

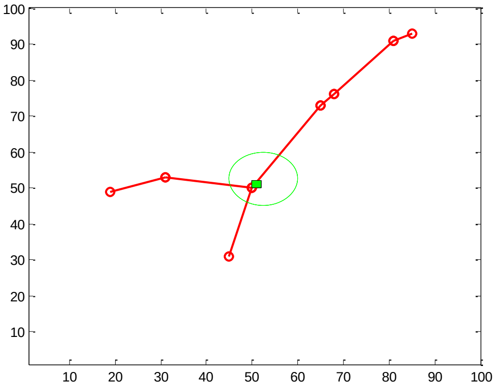

Figure 6. Attack detection results for UCON-IPSO

In the proposed UCON- IPSO algorithm two types of attacks were detected and illustrated in Figure 6. To detect attack in WSN model use Wi-Fi technologies [24]. The membership-based payment policy [25] is used as a case policy for the simulation. To set of connections the simulation for attack detection, we combined UCON- IPSO and Wi-Fi wireless traffic features [26]. Primary, some specific features of UCON are chosen; second, the MAC header field is extracted as the Wi-Fi technology [26]. To calculate the importance of each feature, Information Gain Ratio (IGR) [27-28] is used as a measure. In this section, the simulation results of Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), path delay, Throughput, and Execution Time is measured to compare the existing UCON and the proposed MWQFA-UCON results. In the simulation,

Packet Delivery Ratio(PDR): Packet Delivery Ratio(PDR) is described as the ratio of the number of delivered packet to the destination ,it described as follows.

$$PDR = \sum Number\ of\ packet\ receive / \sum Number\ of\ packet\ send \quad (14)$$

Packet Loss Ratio (PLR): Packet Loss Ratio (PLR) is described as subtracting the value of PDR to 100 to the destination, it described as follows.

$$PlR = 100 - PDR \quad (15)$$

Path delay: It is described the average time taken by a data packet in the direction of arrives in the destination for particular path. It also consists of the delay originate by route discovery stage and the queue in packet transmission. Simply the data packets with the purpose of effectively delivered in the direction of destinations to count.

Throughput: Throughput of a network is able to be determined using many tools available on different platforms. Throughput comparison with respect to time is determined based on the following formula.

$$Throughput = \frac{packet\ received}{amout\ of\ packet\ forward} \quad (16)$$

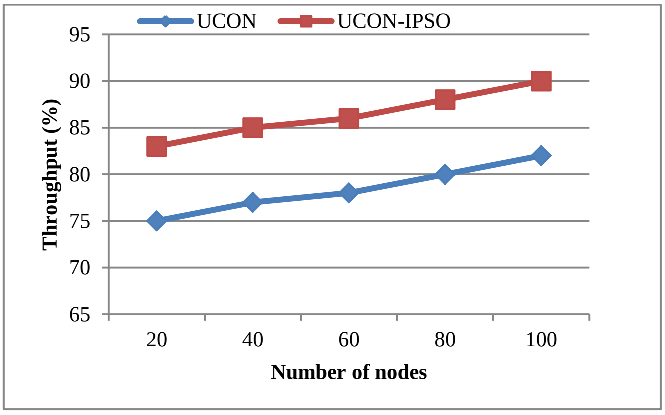

Figure. 7. Throughput results comparison vs. number of nodes

Figure 7 shows throughput comparison results of existing UCON and proposed UCON- IPSO methods. From the results it concludes that the proposed UCON- IPSO framework has provides higher throughput results when compared to UCON if the no. of nodes increases from 20 to 100 tabulated in table 1.

Table 1. Throughput results comparison

Methods/No of nodes	Throughput(%)				
	20	40	60	80	100
UCON	75	77	78	80	82
UCON-IPSO	83	85	86	88	90

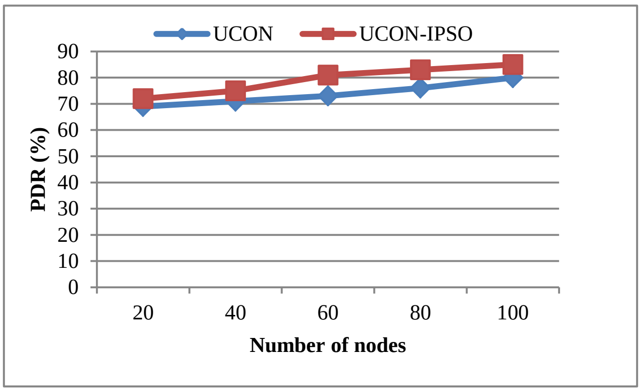

Figure. 8. Packet Delivery Ratio(PDR) results comparison vs. number of nodes

Figure 8 shows PDR results comparison of existing UCON and proposed UCON-IPSO methods. From the results it concludes that the proposed IPSO achieved higher PDR results when compared to UCON if the number of nodes increases from 20 to 100 tabulated in table 2.

Table 2. PDR results comparison

Methods/No of nodes	PDR (%)				
	20	40	60	80	100
UCON	69	71	73	76	80
UCON-IPSO	72	75	81	83	85

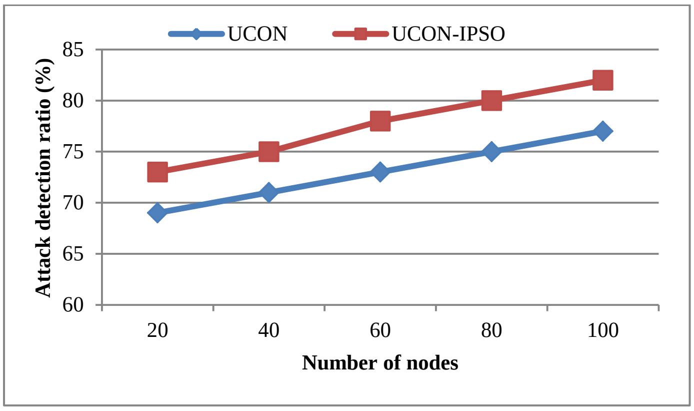

Figure. 9. Attack Detection Ratio (ADR) results comparison vs. number of nodes

The number of attacks detected between proposed UCON-IPSO system and existing UCON system is illustrated in Figure 9. The no. of detected among the time a sensor receives a request and when it makes a local detection decision for proposed UCON-IPSO system is high it is illustrated in Figure 9 and related to table 3.

Table 3. Attack Detection Ratio (ADR)results comparison

Methods/No of nodes	Attack Detection Ratio (ADR) (%)				
	20	40	60	80	100
UCON	s69	71	73	75	77
UCON-IPSO	73	75	78	80	82

5. CONCLUSION AND FUTURE WORK

For WSNs in smart cities, to increase the safety, a new Usage Control with IPSO (UCON-IPSO) hierarchical security framework is proposed which combines the procedure of detection and access control methods. However the proposed UCON-IPSO security framework is extended from the behavior of Usage Control (UCON) with continuous decision making and dynamic attributes. It is useful in defending against ongoing threats. In this work propose an UCON-IPSO security framework is proposed to detect Distributed Denial of Service (DDoS) and Sophisticated Attacks. Finally, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) is proposed for measuring the attack mitigations detects and classified then as either low-level or high-level attacks. Incoming traffic in the direction of the server is continuously monitored in the direction of instantaneously identify any abnormal grow in the inbound traffic. An experiment was performed to measure an attack detection results. The simulation results demonstrated that the proposed UCON- IPSO security framework has higher security and attack detection rate. In the future work we combine attributes of many technologies with continuous decision and dynamic features in UCON are able to solve ongoing attacks with complex persistent threat detection.

REFERENCES

1. Ota, K., Dong, M., Wang, J., Guo, S., Cheng, Z. and Guo, M., "Dynamic itinerary planning for mobile agents with a content-specific approach in wireless sensor networks", IEEE 72nd Vehicular Technology Conference Fall (VTC 2010-Fall), pp. 1-5, 2010.
2. Chang, S., Qi, Y., Zhu, H., Dong, M. and Ota, K., " Maelstrom: receiver-location preserving in wireless sensor networks", In International Conference on Wireless Algorithms, Systems, and Applications ,Springer Berlin Heidelberg pp. 190-201, 2011.
3. Guo, L., Wu, J., Xia, Z. and Li, J., " Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks", IEEE Sensors Journal, 15(5), pp.2577-2586,2015.
4. Dong, M., Ota, K., Yang, L.T., Chang, S., Zhu, H. and Zhou, Z., "Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks", Computer Networks, 74, pp.58-70, 2014.
5. Zhang, R., Zhang, Y. and Ren, K., "Distributed privacy-preserving access control in sensor networks", IEEE Transactions on Parallel and Distributed Systems, 23(8), pp.1427-1438, 2012.

6. Lee, H., Shin, K. and Lee, D.H., “PACPs: practical access control protocols for wireless sensor networks”, IEEE Transactions on Consumer Electronics, 58(2), pp.491-499, 2012.
7. Abdelhakim, M., Lightfoot, L.E., Ren, J. and Li, T., “Distributed detection in mobile access wireless sensor networks under byzantine attacks”, IEEE Transactions on Parallel and Distributed Systems, 25(4), pp.950-959, 2014.
8. Harbin, J., Mitchell, P. and Pearce, D., “Wireless sensor network wormhole avoidance using disturbance-based routing schemes”, In 2009 6th International Symposium on Wireless Communication Systems, pp. 76-80, 2009.
9. Chen, L. and Leneutre, J., “A game theoretical framework on intrusion detection in heterogeneous networks”, IEEE Transactions on Information Forensics and Security, 4(2), pp.165-178, 2009.
10. Lu, W., Tavallaee, M. and Ghorbani, A.A., “ Detecting network anomalies using different wavelet basis functions”, 6th Annual Conference on Communication Networks and Services Research (CNSR), pp. 149-156,2008.
11. Kanoun, W., Cuppens-Boulahia, N., Cuppens, F., Dubus, S. and Martin, A., “Success likelihood of ongoing attacks for intrusion detection and response systems”, International Conference on Computational Science and Engineering (CSE'09), Vol. 3, pp. 83-91, 2009.
12. Lee, H. Y., & Cho, T. H. (2010). A scheme for adaptively countering application layer security attacks in wireless sensor networks. IEICE transactions on communications, 93(7), 1881-1889.
13. Rasheed, A., & Mahapatra, R. N. (2012). The three-tier security scheme in wireless sensor networks with mobile sinks. IEEE Transactions on parallel and distributed systems, 23(5), 958-965.
14. Krontiris, I., Giannetsos, T. and Dimitriou, T. (2008). Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side. IEEE International Conference on Wireless and Mobile Computing, pp. 526-531.
15. Tumrongwittaya and Varakulsiripunth. (2009). Detection of Sinkhole attack in Wireless Sensor Networks, In ICCAS-SICE, 2009 ,pp. 1966-1971.
16. Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, IEEE International Conference on Wireless Communication, Networking and Information Security (WCNIS), pp. 711-716.
17. Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management. IEEE Symposium on Computers and Communications (ISCC), pp. 537-542.
18. Coppolino, L., D’Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. 5th International Conference on Critical Infrastructure (CRIS), pp. 1-8.
19. Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. 5th IEEE Workshop on Secure Network Protocols, 2009 (NPSec 2009),pp.43-48.
20. Fessant, F., Papadimitriou, A., Viana, A.,Sengul, C. and Polamar, E. (2011) A sinkhole resilient protocol for wireless sensor network: Performance and security analysis. Computer Communications, 35(2), 234-248.
21. Sheela, D., Kumar, N., and C Dr. Mahadevan, G.C.(2011). A non-Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks. International Conference on Recent Trends in Information Technology (ICRTIT), pp.527-532.
22. Y. Shi, R.C. Eberhart, Empirical study of particle swarm optimization, in: CEC99. Proceedings of the 1999 Congress on IEEE Evolutionary Computation, 1999.
23. Dingwei Wang, Wang Junwei, Wang Hongfeng, Zhang Ruiyou, Guo Zhe, Intelligent Optimization Methods, Higher Education Press, Beijing, 2007, 221–226.
24. G. Anastasi, E. Borgia, M. Conti, E. Gregori, and A. Passarella, “Understanding the real behavior of Mote and 802.11 ad hoc networks: An experimental approach”, ' Pervasive Mobile Computing., vol. 1, no. 2, pp. 237-256, 2005.
25. Karaboga D., An Idea Based On Honey Bee Swarm for Numerical Optimization, Technical Report TR06, Erciyes University, Engineering

Faculty, Computer Engineering Department, 2005.

26. J. Park and R. Sandhu, “The ABC core model for usage control: Integrating authorizations, obligations, and conditions”, ACM Transaction Information System Security., vol. 2, no. 3, pp. 1-46, 2002.
27. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer Extension in the 2.4 GHz Band, IEEE Standard 802.11-1999, 1999.
28. J. R. Quinlan, “Induction of decision trees”, Mach. Learn., vol. 1, no. 1, pp. 81-106, 1986