Ontology based Intrusion Detection System in Wireless Sensor Network for Active Attacks

Maruf Pasha
Department of Information Technology
Bahauddin Zakariya University
Multan, Pakistan

Naheed Akhter
Department of Information Technology
Bahauddin Zakariya University
Multan, Pakistan

***Abstract*—WSNs are vulnerable to attacks and have deemed special attention for developing mechanism for securing against various threats that could effect the overall infrastructure. WSNs are open to miscellaneous classes of attacks and security breaches are intolerable in WSNs. Threats like untrusted data transmissions, settlement in open and unfavorable environments are still open research issues. Safekeeping is an essential and complex requirement in WSNs. These issues raise the need to develop a security-based mechanism for Wireless Sensor Network to categorize the different attacks based on their relevance. A detailed survey of active attacks is highlighted based on the nature and attributes of those attacks. An Ontology based mechanism is developed and tested for active attacks in WSNs.**

Keywords—Semantics; Wireless Sensor Network; Intrusion detection and prevention system; ontologies

I. Introduction

Wireless sensor nodes have reorganized not only the process but also the strategy structure of any system; either identifying any person in moving groups, or tankers in the battle field, pollution in surroundings, determining the stream of traffic on transportations, as well as mark out the worker's position in office block. Several WSNs are used in critical applications and consequently they need active security alerts [2][3][16] wireless sensor Network offered great suppleness in data broadcast but there are a quantity of matters of security in sensors node owing to restricted resources such as processing unit and power . Invader can take passive and active attacks skills. Possible attack in WSN can be DoS, Jamming, Sybil, Wormhole, Tempering, Selective Forwarding, Sinkhole, Hello Flood Attacks, and Acknowledgment Spoofing.

WSN has most important challenges in operating security arrangements due to wireless medium, Ad-Hoc Deployment, Unreliable Communication, Unreliable Transfer, Conflicts Latency, Unattended Operation, Exposure to Physical Attacks Managed Remotely. In WSN security requirement can be achieved by applying Authentication, Integrity, and Data Confidentiality, Data freshness, Availability, Self-Organization, Time Synchronization, Secure Localization, Nonrepudiation. This work implements ontologies to improve the IDS in WSN.

Ontology can be used to classify and infer new knowledge by identifying the relevance among different attacks, The work focuses on categorization of new nodes in ontologies and then these relations of nodes are then applied to detect malicious activities.

After placement of the WSN, BS gathers routing and positioning information of sensor nodes. At earlier stage of IDS select the cluster head node highest energy based, two agents that have low energy status in respect of CH and starts the abstract relationships of each node in the ontology. The broadcast of every node will be governed by its association to the ontology. The intruder cannot then make-believe that nasty nodes are legal nodes.

The proposed architecture is divided into five sections. (1) Data routing information, attack threshold/feature. (2) Data gathering and monitoring cell depending on the environment. (3) Agent system that collect data from monitoring/ collection cell and check its status, also decide the behavior of data. (4) Knowledge Management System

Ontology, SWRL Rules, Attack Signature section construct ontology properties, set threshold relationship match SWRL Rules and attack signature. (5) IDS Section Analysis data & decide which attack type and produce alert system.

This paper is structured as Section I introduction. Section II Semantic based Architecture. Section III Approach used to detect attack in WSN. Section IV Related Work. Section V Proposed methodology. Section VI Proposed Security Ontology. Section VII Result and evaluation. Section VIII conclusion and future direction.

A. *Major Challenges in Sensor Network Security*

The natural surroundings of all sorts of networks appear the unique contests in manipulating security schemes. WSNs is a distinct sort of network which has additional restrictions than any other old networks [4][8].

Wireless Medium

The wireless medium is basically unsecure due to its broadcasting nature. Thus any challenging can straightforwardly stopped, altered and rerun the broadcast [8].

Ad-Hoc Deployment

The placement of ad-hoc in SNs results that not fix discrete structure. The network topology altered frequently and difficulty to identify.

UNRELIABLE COMMUNICATION

Major warning on sensor security is unreliable communication.

UNRELIABLE TRANSFER

The transmitting of packets is unreliable due to connectionless channeling is used in WSNs.

CONFLICTS

Due to broadcast nature of WSNs might be substandard communication while a trustworthy channel exists.

LATENCY

There could be enormous latency in the network because of network blocking and multi hop routing.

UNATTENDED OPERATION

When directing the functionality of specific WSNs, sensor nodes may be unattended for a long period of time [9].

EXPOSURE TO PHYSICAL ATTACKS

The WSNs Sensor nodes placed in open environment due to this that it is easily visible to the adversaries. The ratio of facing physical attacks in sensor networks is significant higher than typical computer systems [10].

MANAGED REMOTELY

WSNs are control remotely so that it is difficult to maintain and find out the physical intrusive in the network.

B. *Security Requirements*

The security requirements of all WSNs can be characterized as follows [11][12]:

AUTHENTICATION

In process of communication or exchanging of switching information trustworthy authentication between sender and receiving sensor node is required.

INTEGRITY

An unauthorized or an invader can be altered data during the transference process by the illegal access. Integrity in information guarantees that information is safe or not once transformed or alter during transference.

DATA CONFIDENTIALITY

Some applications need dependency on confidentiality. Some applications are key distribution, data surveillance system as well as industrial secrets. Encryption is a standard technique for assuring confidentiality.

DATA FRESHNESS

In Security Requirements verifying the data must be fresh and not repeating the previous messages when mutual keys are recycled in WSNs. In this incident possible adversary can originate an attack with usage of old key [13].

AVAILABILITY

There is a big issue of limited battery power. In huge communication therefore the Sensor nodes become absent. Unavailability of nodes can happen due to battery power expiration that an intruder may blocked the communication. The security requirements must assure the sensor node availability.

SELF-ORGANIZATION

In WSN, each sensor node is self-governing, random deployment and abundant to be self-healing affording to different disturbance environments, no fixed infrastructure, and support multi hop [7][9]. There is deficiency of an individual infrastructure in Wireless Sensor Networks because all sensor nodes in the Networks are self-governing and establish randomly as well as each node has the feature of self-curing due to numerous hassle environments. There is essential need of self-organized networks of nodes to keep up multi hop routing.

TIME SYNCHRONIZATION

Some security method accessible to bring together the sensor nodes to make Wireless sensor Networks time-synchronized due to any node might be shut down to save power.

SECURE LOCALIZATION

WSNs repeatedly need information around the position of sensor nodes suitably as well as unavoidably. An attacker can basically switch the information of doubtful place with help of broadcasting false strong point of signals as well as replaying the indications etc.

NONREPUDIATION

It illustrate that sensor node cannot discard to send the communication if the message directed before. Moreover we recommend the forward and backward secrecy.

- Forward secrecy: When a sensor node leaves the sensor network it cannot deliver any longer the upcoming messages.
- Backward secrecy: A fresh joined node may not be capable to deliver any of the previous communicated messages.

C. *Threat Model*

Ordinarily expected that an intruder might identify the procedures of security planned in WSNs or may be captured a sensor node actually. Due to organizing high charge sensing nodes. There may be few nodes seems to be compromised nodes, with the help of compromised node an invader with no trouble access the key resources.

Attacks in WSNs can be distributed into the following groups [14]:

- The attacks can occur from inside or outside the network. Outside side attacks takes from sensor nodes not from sensor network. While an authentic sensor node performed negative activities or break communication law taken as insider attack.

- In passive attack attacker scanned exposures and open ports of the sensor network without communication by catching the session ID or engage the sensor nodes by skimming its ports.
- However the active attacks contain some types of adjustments of data flow or construction of immoral data flow.
- In mote-class, an attacker attacks the wireless sensor network with the support of few nodes which have identical abilities to the sensor nodes.
- Laptop-class attacks, the intruders might have greatly powerful devices, which have too much control for processing, higher range for broadcasting as well as replacement a percentage of energy as equated to the nodes of WSNs.

D. Evaluation

Few metrics could be used to discover the appropriateness of security system inside sensor network [11]:

Security: A security technique should achieve the simple needs.

Resiliency: The security device should protect the attacks.

Energy Efficiency: Security device should also authenticate the energy effectiveness in order to exploit the lifespan of the wireless sensor network.

Flexibility**:** Key management should be flexible in order to authorization multiple network organization methods like uninformed scattering of sensor node as well as commitment of arranged node.

Scalability: Security tool should adept to scale the security needs.

Fault-Tolerance: Security tool should adept smooth and accurate transmission for communication throughout the incidence of fault nodes.

Self-healing: The security device must be self-healing as nodes should be able to reposition in case of network failure.

Assurance: The arrangement of security must be capable to recommend varieties with respect to ideal reliability, latency etc. The security technique should fulfill the assurance of dividing information to different users [15].

E. Attacks in sensor networks

Attack can be identified signature based or anomaly based. In different work attack can be sensed in diverse techniques such as

- **Hello Flood**, wormhole attack occurs due to power strength difference of signal in WSN.
- In **DoS** attack attacker used garbage value that a sensor node accept false value.
- The **jamming** attack take place with delays inside the frequencies.
- In **tempering** attack an invader has physically accessed to any node in the WSNs to get information about security keys
- In **Spoofed, Replayed and Altered** attacks attacker straightforward targeted on routing protocol in WSN while swapping data between nodes.
- **In Selective Forwarding** an invader can create bogus nodes which only sending the choosy messages and drop others
- In **black hole** attack attacker drop all the data packets that sensor node expected.
- In **sinkhole attack**, an invader with the help of a fake node appearances attracting to all other neighboring nodes in order to get the routing information.
- In **Sybil attack** the invader used many identities in a sensor network.
- In **Wormholes** attack occur due to low-latency link in WSN.
- **Hello flood** a**ttacks used** HELLO packets to consume the energy of other sensor nodes by making artless supposition that the source node is the neighbor range.

II. Semantic based Wsn Architecture

Depending upon heterogeneity in System, Structure, Syntax and Semantics data Integration is a difficult task. OWL/RDF used to describe the sensor services. Sensor/Monitor Node used IEEE 1451 Standard for categorizing data and information link. Web service called using WSDL based on XML format. RDF describe relation in triples “Subject + Predicate + Object”. Ontology is a “*formal specification of a shared conceptualization*”. User gets web services using registry request type public or private using UDDI. SOAP protocol used for switching building information in web services. Jena API used to extract statistics from and create graph in RDF/OWL format, which queried through SPARQL.SWRL rules used for system behavior analysis is a normal or a malicious.

III. Approach used to Detect Attack in Wsn

A number of security procedures used to distinguish the information based, pattern based, and rule based, formal based and heuristic conceptions and combination of these technique attacks through IDPS. IDPS categorized into three types Application based, Host-IDS and Network-IDPS. due to knowledge base in Semantic Web attack divided into two categories (i) Detectable (ii) Undetectable. Non-ontological approach can only detect detectable attacks which is not efficient approach because signature of any attack can be easily modify. Ontology approach is stretchy to describe any perception at any level and can be used and shared between different individuals within domain. Ontology reduce large variation of sets into a list of properties.

IV. Related Work

In different research used different tools to detect attack such as DAML + OIL (DARPA Agent Markup Language), DAML Jess KB and for security assumption used UPML Unified Problem Solving Method Description language. In another work used (Descriptive Logic based Web Ontology Language) OWL-DL for attack detection due to expressiveness and full inference support. In [17] attack occur in Semantic web are XML, SQL, XPath Injection attacks, SOAP attacks, UDDI attacks. DoS attacks, XSS attacks, Application attacks.

In mostly research used layered approach to detect attack in WSN. In [1] used four layers and use Co-Operative Intrusion Detection Algorithm which based on number of different agents. In [16] used two layers and use Co-WIDP (Collaborative-based wireless IDPS) technique.

In [5] used Rough Set Theory and Sport Vector Machine to detect attack. In [6] used different IDS System to detect attack i.e. Target Centric Ontology, Outbound ID Architecture and semantic Ontology. In [18] used SUMO (**Suggested Upper Merged Ontology)** and IEEE 1451 Transducer used for Sensor Network which merged three ontology SHO (**Sensor Hierarchy Ontology),** SDO (**Sensor Data Ontology)** and EPO (**Extension Plug-ins Ontologies)**. In used Agent based Simulation Novel Approach used to detect DDOS in any critical Infrastructure with anticipation game which depend on four thing Dependency Graph (Network Services, a set of attributes (States) , rules, policies and Communications proceeds between the attacker and the protector.

V. Proposed Architecture

F. *Overview of the planned model*

IDPS classified such as

- Application based IDS detect intrusion in a particular application protocol.
- Host-IDS has single node user log info etc.
- Network-IDPS has info about flows, data packet and protocol activities in specific network section.

Attack can be discovered signature based or anomaly based.

In some previous research work used Fuzzy reinforcement Learning Management, security ontology, Knowledge management and multi Agents System to monitor, analyze and collect audit data through sensor Node and detect intrusion through complex technique. However if number of agents is more than maximum delay occur.

In our proposed architecture we expand the security ontology design by covering the relation sets concluded properties and distinguish diverse attack sort such as **active or a passive** attack and associate attack type. Also reduce their attack exposure time and create the semantic based WSN-IDPS Architecture. The proposed architecture is arranged into three parts.

1. Agent System and Security ontology.
2. SWRL Rules.
3. Ontology workflow.

This presents the anticipated design of WSN to detect attack. In our system at section 1 configured WSN routing information and WSN attack packages/sets, section 3 agent system consist two agent common agent and monitor agent. Common agent collects data from section 2 and patterned its status Section 3. Section 4 match malicious activity pass this report to monitor agent which inquiry to security ontology and decide the actions of data, useful data than permit it to go the prerequisite Sensor Node or else decided about the attack signature, section 5 develop IDS and update the section 1 and generate alert system to user. Fig. 1 presents the proposed architecture,

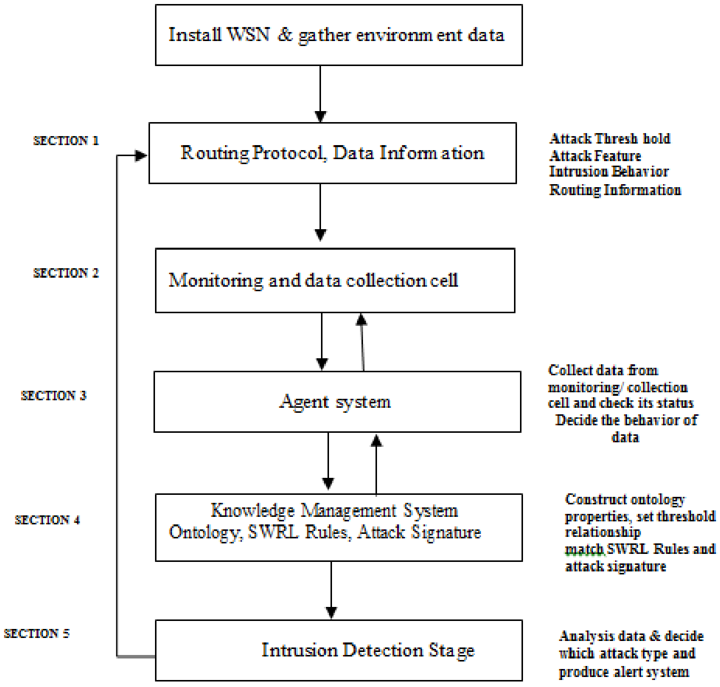


Fig. 1. Proposed Architecture

To develop agent system used Jade, Java Agent Development Framework. To create relations between Agents and security ontology used Jena, Java framework for constructing WSN Architecture, to create graph in RDF/OWL format, which queried through SPARQL.

VI. PROPOSED SECURITY ONTOLOGY

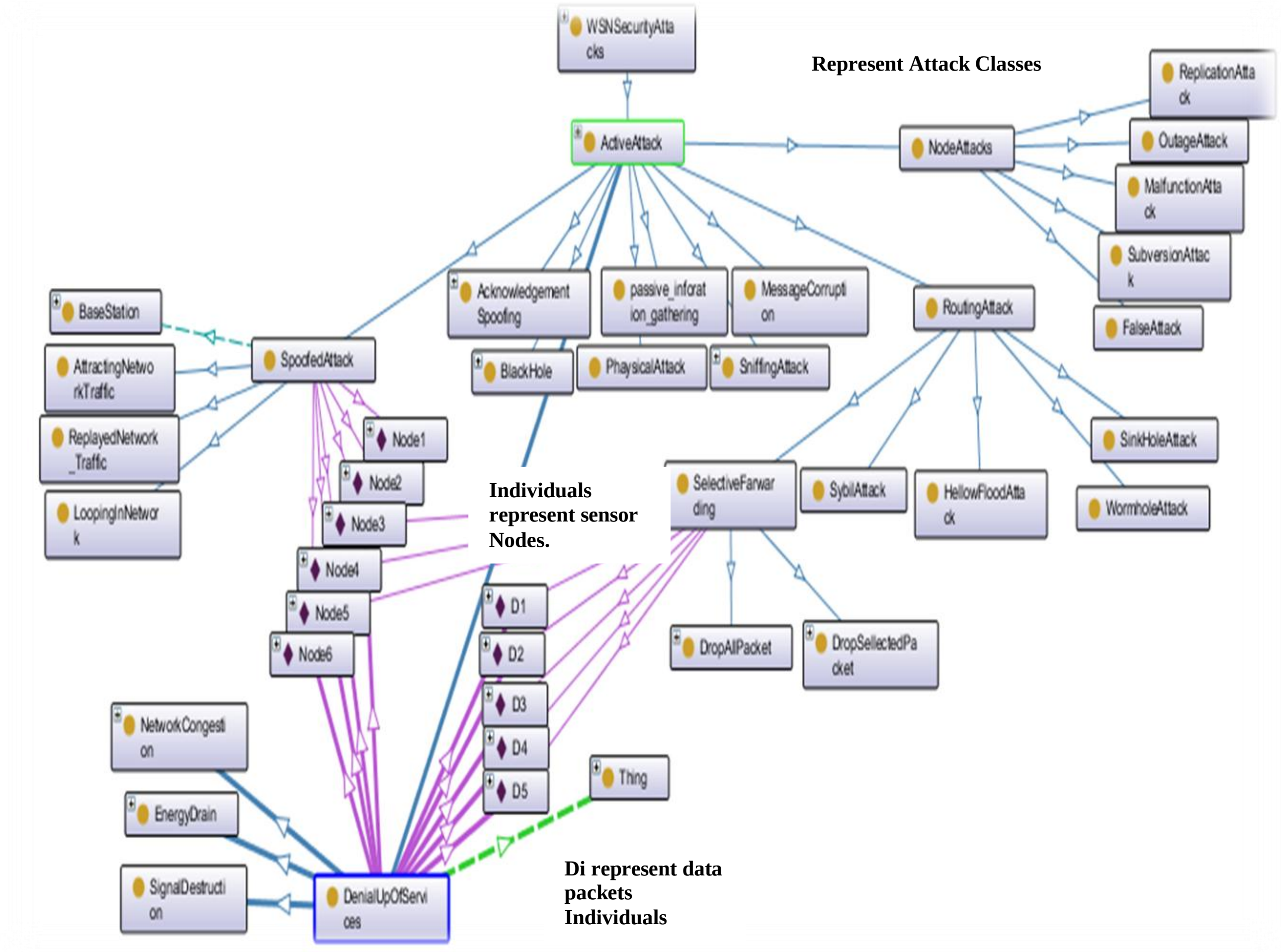
After in depth analysis of Wireless Sensor Network domain, we conclude that the web Semantic based WSN ontology is the appropriate to identify the diverse WSN attack.

Attack ontology can be built by studying special domain or reused/rebuild previous ontology accessible in that domain to complete. Intrusion Detection System has insufficient ontologies. Attacks can be classified into two groups: active and passive attack**s.**

a) Active Attacks

In Active attack groups attacks are Acknowledgment Spoofing. Black Hole, Message corruption, physical attack, sniffing attack , in routing attack hello flood , selective forwarding, sinkhole , Sybil attack wormhole, Node attack, and in DoS hello flood, energy drain. Network congestion, jammers.

We build our recommended ontology by using open source Protégé. Fig. 2 shows the upper level classes of Active Attacks, data individuals and sensor nodes individuals.



Represent Attack Classes

Individuals represent sensor Nodes.

Di represent data packets Individuals

Fig. 2. Active Attack

b) Passive Attack

In passive attack invader scanned vulnerabilities and open ports of the system without interaction by capturing the session ID or engage the system by scanning its ports. Invader used war driving, antenna and GPS system and dumpster diving method used to attempt such type of the attack. The main purpose of this attack is to get information around the target like traffic analysis and no data is altered. Passive attacks are preliminary actions for doing active attacks. Figure 2 shows the upper level classes of passive Attacks. Passive attack IDS beyond our work.

Passive attacks are traffic analysis, Monitor and eavesdropping, MAC Protocol and camouflage adversary.

VII. INTRUSION DETECTION ALGORITHM

In our scenario used six Sensor Nodes $_{(I)}$ and assign each node an ID for authentication and session ID for communication. First we set the **threshold Value** to detect different type of attack in ontology.

A. Symbol used for proposed Algorithm

Sensor Nodes NID [ ], Monitor Node MID [ ], Energy Status E-fi, for Radio Communication Range used RCR and sensed data kind info SDT, resources of sensor Node used RSN [ ] , for communication session information such as starting time, data transmission time and communication completion time store in time[ ] and for isolation table used IT[ ].

B. Intrusion Detection Stage

The intruder that intrude wireless sensor network into two phases:

- Initial attack phase about attack behavior
- Destruction phase about attack type.

The intruder used various programing ability to burn comprehensive network, even marks WSN unfeasible. These activities are called anomaly acts. The ontology covers the comprehensive relationship of the WSN. The common nodes transport section of ontology and Monitor Node contest the SWRL rules to detect different sorts of attacks.

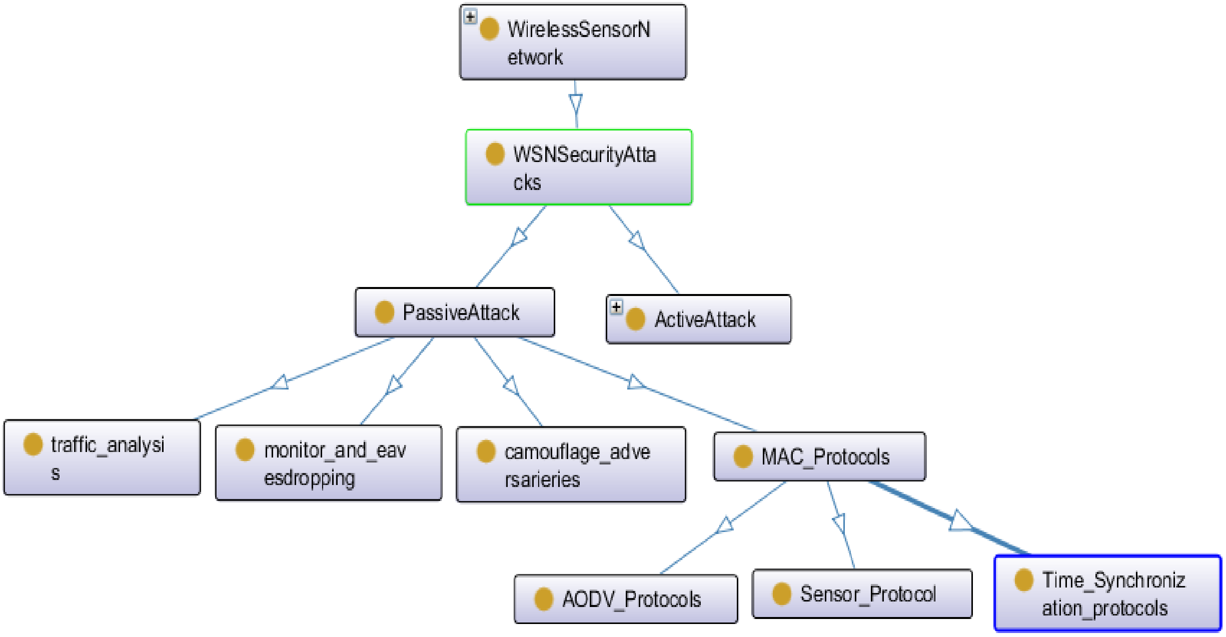


Fig. 3. Passive Attack

C. Algorithm to detect different attacks in WSN

Input: The WSN communication packages and attack packages

Output: MID list of Malicious Nodes MID[]

- Pre-processing and broadcasting routing Stage

```
for each Sensor Node SN attached to N do
/*where N represent a particular WSN Segment*/
for each sensor node $S_j$ in the network do
if $D_{SN}[S_j] + S_{ID}(N, s_i) < D_N[S_j]$ then    /*here D represent distance information of a sensor Node*/
/∗a better route from N to $S_j$ through SN has been found∗/
$D_N[S_j] \leftarrow D_{SN}[S_j] + S_{ID}(N, s_i)$.
$CH_N[S_j] \leftarrow$(N, SN)
 /* CH represent the cluster head of a network segment*/
for each Sensor-Node SN transmitted to Base-station BS do
Send data of itself $S_{ID}$ to base station BS
return $S_{ID}$   /* Info about Sensor Node ID*/
```

- Concept to build Ontology Stage

```
/∗ sort sensor nodes in respect to energy status ∗/
for each sensor node SN in the network do
for ($i = n - 1; i > 0; i - -$) do
for ($j = 0; j < i; j$++) do
if energy($SN_j$) > energy($SN_i$) then
/*NID represent Sensor Node in network*/
buffer = NID[$j$]
NID[$j$] = NID[$j + 1$]
NID[$j + 1$] = buffer
return NID[]
/∗ return sort information of active Node in WSN ∗/
/∗ this arrangement selects best sensor node as a Cluster Head in particular Network Segment and in NID[ ] array at index “0” Sensor Node has highest energy status ∗/
set CH = NID[0]
/∗pick up next two Sensor Node as a Monitor nodes∗/
```

```
for (m =1; m< $n$ ; m++) do
 /*here the value of n is less than "3" */
MID[m] = NID[m]
/∗ pick up two sensor nodes as a monitor node which are at index 1 and 2∗/
for each sensor node $S_{ID}$ in the MID[] do
if hop($SN_i$, CH) = 1 then
/∗a Monitor node has found∗/
set MID[] = $SN_i$
```

- Construct Monitor nodes in Ontology

```
for each Monitor node in the network do
for (m =1; m< $n$ ; m++) do
 /∗ m is the index of Monitor node ∗/
/∗ $MN_i$ ∩$MN_j$ compare the data of MN  and $MN_j$ to collect the lowest number of source such as energy-status ( ), hop ( ) and sense-data-type ( ) etc. $MN_i$ U $MN_j$ calculate the data of $MN_i$ with the statistics of $MN_j$ to collect the smallest number ∗/
$t_m$ = intersection ($MN_i$, $MN_j$) / union ($MN_i$, $MN_j$)
$MN_j$[] ⟵ $MN_i$
Ontology[] ⟵ $MN_j$[]
```

- Relationship b/w Sensor Nodes

```
for each Sensor-Node $SN_{ID}$ in the network do
if $SN_i$ <> $SN_j$ and resource($SN_i$) ≠ resource(SNj) and hop($SN_i$, SNj) = 1 then
/* $SN_i$ , $SN_j$  are two differ Node, resources are different and distance b/w them is same from one hop and $MN_i$ managed these sensor nodes*/
/∗ an equivalent sensor Node has initiate ∗/
set $SN_i$ , $SN_j$ are equivalent sensor nodes
for each Sensor-Node $SN_{ID}$ in the network do
if $SN_i$ <> $SN_j$ and resource($SN_i$) ≈ resource($SN_j$) and 2 ≦ hop($SN_i$, SNj) ≦ 3  then
/* $SN_i$ , $SN_j$  are two differ Node , resource are same and distance b/w them is "2" then differ Monitor node are on same level and have sister co-relation or less than and equivalent to "3" from one hop then have sibling co-relation and it will be adjusted conditionally on the scale of WSN  */
/∗a sibling sensor Node has found∗/
set $SN_i$ and SNj are sibling Sensor Nodes
else if Monitor-Node($SN_i$) ∩ Monitor-Node(SNj) <> then
set $SN_i$ and $SN_j$ are sibling sensor nodes.
```

- Construct Ontology

```
for every SN in the network do
for (i = 1; i≤ $n$; i++) do  /∗ i is the index of Monitor Node ∗/
$t$i = intersection ($MN_k$, $SN_i$) / union ($MN_k$, $SN_i$) /∗$t_i$ is sister co-relation of Monitor Node i ∗/
$t$ = $t$ + $t_I$    /∗$t$ indicate the sister or Sibling term ∗/
return $t$
Monitor-Node ($MN_k$, $SN_i$) = $t$/i
$MN_i$[] ⟵ $SN_i$
Ontology[] ⟵ $MN_i$[]
```

- Intrusion Detection Phase for physical Node, false Node, Node Malfunction, Sink hole, Sybil attack, Hello flooding and black hole attack

```
**for** each neighbor Sensor Node of Monitor Node  **do**
receive ($SN_{ID}$, $MN_{ID}$, $SN_{INFO}$, $E$_fi)
/∗ Receive $SN_{ID}$, $MN_{ID}$, $SN_{INFO}$ and the remaining energy ∗/
if $S_{ID}$ <> $Ontology$ [] then
/∗ Checked whether the sensor node is built in the Ontology ∗/
then $A$N[] = ($SN_{ID}$, $MN_{ID}$, $A$N)
 /∗ Record $SN_{ID}$, $MN_{ID}$ and anomaly information ∗/
if Pattern ($SN_i$) ! = Pattern ($A$N)
/∗ Check whether the receive information is different from attack knowledge ∗/
    then $A$N[] = ($SN_{ID}$, $MN_{ID}$, $A$N)
     /∗ Record $SN_{ID}$, $MN_{ID}$ and anomaly information ∗/
else if broadcast $A$N[] to CH /∗ Broadcast isolation table to CH and update anomaly and signature database information for back up ∗/
end for
```

- Wormhole, Acknowledgement Spoofing attack, black hole, Message corruption, sniffing attack, signal destruction/jammers and Routing attack detection phase

This **wormhole** attack can be detected by data packets are saved in Monitor Node buffer when sender and receiver Node exchange data packets with each other and also keep record of time threshold of each data packet to verify the correct information of Monitor Node. Check information status in buffer. AN[i] maintained of each Monitor $Node_{id}$ and keep record of each Monitor Node sliding window MN_{S_Window} . Monitor Node keep record of its nearest sensor node. Monitor Node explored logical position of sensor node. However in WSN adjacent node may be alteration their position during lifetime of network. So dynamic detection required. Malicious Node easily detected because each sensor node record exist in ontology. When a sensor node receives the request channeled by a malicious node it append the identity of malicious node or its neighbor node. It can also be detected due to it has no packet information of SN_j in its buffer.

/* Authentication process b/w $Node_i$ and $Node_j$ */

for each Sensor Node SN attached to N do

/*where N represent a particular WSN Segment*/

/* Radio Communication Range used RCR, resources of sensor Node used RSN [], for communication session information such as starting time, data transmission time and communication completion time store in time[ ] and for isolation table used IT[ ].*/

1) for each sensor node SN_j send message MN_i with the time[] to SN_j which expects with RCR, to in the network do.

2) MN_i encrypt SN_i request using public symmetric key.

3) MN_i check its Routing Table for SN_i to verify SN_i has no previous valid communication session. And SN_j has not already revoked. If SN_j has already authenticated then

Monitor Node drops the handshaking request by private key sending back to SN_i.

4) If step 3 do false, Monitor Node send Acknowledgement that contain the id of $SN_{i,}$ session expiration time[i] , this time equal to the Monitor Node handshaking request time for authentication and new location information of Node SN_j and send back to SN_i.

5) When SN_j receive the result of authentication process than SN_j acknowledgement through public key to Monitor Node.

6) If Monitor Node reject the SN_j request, then every Sensor Node in this network segment reject the communication request of SN_j and add his path address to isolation table IT[].

7) If position remained same in Authentication process and communication time is not expired than a Sensor Node can send, forward and receive data packets.

8) If current position is changed from authentication process and time limit expire than a Sensor Node cannot send, forward and receive data packets.

9) SN_j send broadcast hop for its authentication, than authentication process determine its neighbor Sensor Nodes

*10)*Neighbor SN_i accept the detection of authentication and proof the initials of Monitor Node and its future communication session, again collect the clock synchronized time information and compute hop distance of SN_j and add it as its neighbor Node list along his current position and store SN_j position.

11)SN_i directs its own authentication using shared key to SN_j along its local malicious Node list MN[] .

12)SN_j verified the authentication of SN_i using the initials of Monitor Node and its communication session time and update its neighbor sensor node list and computed distance of SN_i and its own location and store the malicious node list of SN_i

*13)*When SN_j complete or expired its communication process than SN_i remove SN_j to its neighbor Sensor node list.

VIII. Results and Evaluation

The results detect main assessment criteria, the particulars of data set, the attack structure; system specification and final results of the research approved complete the system.

- System Specification
- Core i5

• System Processor	• Intel® Core (TM) i5 4010U CPU @ 2.70 GHz
• RAM	• 4GB
• HDD	• 500GB
• Operating System	• 64 bit Windows 8.1
• Tool	• Protégé, Java

Sensor Node Concept in Ontology

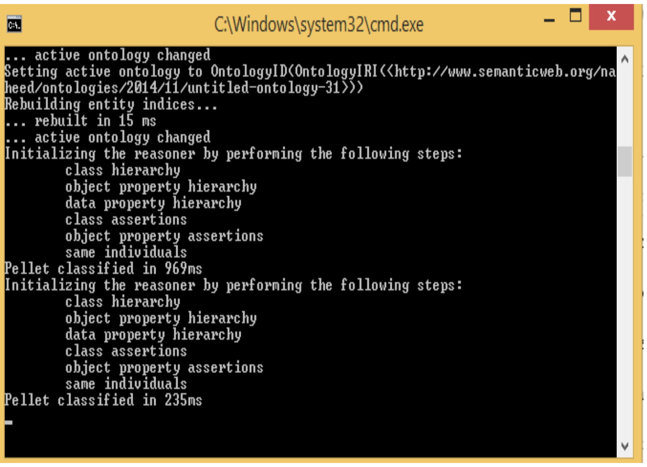
The ontology data consist of sensor node ID, Monitor node ID, energy in joule, hop distance and sensing data type i.e. temperature, humidity, Brightness.

TABLE I. Node Status

Node Type	Energy level in joule	Hop
Cluster Head	Top most energy	1
Monitor Node	89% to 80%	2 to 3
Sensor Node	below 80% to 30%	4 to above
Dead Node	below to 30%	---
Attacker Node	Use Threshold value	

Implementation environment

• Sensor nodes	10
• Monitor nodes (20% of SN)	02
• WSN size	1000 ∗ 1000m^2
• Starting energy	2 joule
• Transmission radius	100m
• Transmission consumption	0.072w
• Receive consumption	0.048w



```
... active ontology changed
Setting active ontology to OntologyID(OntologyIRI(<http://www.semanticweb.org/na
heed/ontologies/2014/11/untitled-ontology-31>))
Rebuilding entity indices...
... rebuilt in 15 ms
... active ontology changed
Initializing the reasoner by performing the following steps:
        class hierarchy
        object property hierarchy
        data property hierarchy
        class assertions
        object property assertions
        same individuals
Pellet classified in 969ms
Initializing the reasoner by performing the following steps:
        class hierarchy
        object property hierarchy
        data property hierarchy
        class assertions
        object property assertions
        same individuals
Pellet classified in 235ms
```

Fig. 4. Pallet inferences

Security Ontology Metrics and class axioms include 66 classes with constrained time inference. Pellet conclusion engine categorized between class, object, data property hierarchy, class assertion, same individuals in 969ms 1st time and 2nd time classified near about 235ms shown in figure 3.

The total time of Simulation was 1800 sec on prowler simulator. Attacks were unsystematically performed every 15 sec with attacks start at 300 sec. To assess the presentation of the system, succeeding formulas and technique are recycled to measure system accuracy:

- Number of Normal communication Records: NCR
- Number of Attack Records during transmission: NAR
- False Positive Attack (mean attack detection signature based): FPA

- False Negative Attack (Mean attack detection Anomaly profile based): FNA
- Detection Rate Percentage = [(NAR-FNA)/NCR]*100
- False Alarm Rate Percentage = [FPA/NCR]*100

IX. Conclusion and Future Directions

We have given a detailed analysis of results and upcoming directions where the proposed work can be used. A foremost conclusion is that the outcome of ontology can be surveyed in the wireless sensor network attack detection. The results show that the ontologies can be used in Wireless Sensor Networks to detect attacks successfully. This indicates that an ontology specifying each role and its individuals in the Wireless Sensor Network could be developed for different attack types.

This work leads to an ontology based ID-System which agree to us to study the relationship method concerning Monitor Node status and Common nodes. More than one ontology is used to reduce or detect attacks in ID-Systems in wireless sensor networks. Overall, they will be suitable in refining the lifecycle of WSNs and, mainly usability to detect different attacks for wireless sensor networks. Contributions of the research involve involvement of the suggested methodology for semantic interoperability throughout the process of communication in WSN. The correct assessments of the system tested through Algorithm of the Semantic base Intrusion detection System for Wireless Sensor Network. The passive attacks security concern will be resolved in the future work.

References

[1] A Semantic-based Intrusion Detection Framework for Wireless Sensor Network Published in Networked Computing (INC), 2010 6th International Conference by Yuxin Mao.

[2] H. Chan and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., p. 103–105, 2003.

[3] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 06, p. 38–43, 2004.

[4] S. Naeimi, H. Ghafghazi, C.-O. Chow and H. Ishii, "A Survey on the Taxonomy of Cluster-Based Routing Protocols for Homogeneous Wireless Sensor Networks," Sensors, vol. 12, 2012.

[5] Ranger Intrusion Detection System for Wireless Sensor Networks with Sybil Attack Based on ontology new aspects of applied informatics, biomedical electronics & informatics and communications.

[6] Ontology-based Distributed Intrusion Detection System Abdoli,F.;Kahani,M. Publication Year: 2009 Proceedings of the 14th International CSI Computer Conference (CSICC'09)

[7] A. Jain, S. Deepak, G. Mohit and V. A. K., "Protocols for Network and Data Link Layer in WSNs: A Review and Open Issues," Advances in Networks and Communications, Communications in Computer and Information Science, vol. 132, pp. 546-555, 2011.

[8] T. Naeem and K.-K. Loo, "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks," International Journal of Digital Content Technology and its Applications, vol. 03, no. 01, pp. 89-90, 2009.

[9] J. P. Walters, Z. Liang, W. Shi and V. Chaudhary, "Wireless Sensor Network Security: A Survey," Security in Distributed, Grid and Pervasive Computing Yang Xiao, vol. 10, no. 15, pp. 3-5, 2006.

[10] A. Pathan, H.-W. Lee and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in The 8th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, 2006.

[11] G. Bianchi, "A comparative study of the various security approaches used in wireless sensor networks," International journal of advanced science and technology," International journal of advanced science and technology, vol. 17, no. 01, pp. 31-44, 2010.

[12] T. A. Zia, "A Security Framework for Wireless Sensor Networks," 2008. [Online]. Available: http://ses.library.usyd.edu.au/ bitstream/2123/2258/4/02whole.pdf. [Accessed 10 December 2014].

[13] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03), San Francisco, CA, 2003.

[14] J. Deng, R. Han and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Department of Computer Science, University of Colorado, Tech. Report, Colorado, 2003..

[15] B. Deb, S. Bhatnagar and B. Nath, "Information Assurance in Sensor Networks," in 2nd ACM Int'l. Conf. Wireless Sensor Networks and Applications (WSNA '03), San Diego, California, 2003.

[16] An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique by Shahab shamshirband Publication Year: 2013

[17] Security Solution for Semantic SCADA Optimized by ECC Mixed Coordinates 2012 International Conference on Information Technology and e-Services by Sahli Nabil, BenMohammed Mohamed.

[18] A Universal Ontology for sensor networks Data by Mohamad Eid, Ramiro Liscano , Abdulmotaleb Ei Saddik Publication Year: 2007