THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-14-December-2019

A Survey on Defense, Detect and Defeat against Selective Forwarding Attack in Ad-hoc Wireless Sensor Networks

Mr. A.V.S.Sudhakara Rao[1] Dr. M.Sreenivasulu[2]

1. Research Scholar, Department of Computer science and Engineering, JNTU Ananthapur, Ananthapuramu, andesudhakarrao@gmail.com.
2. Professor & HOD, Department of Computer Science and Engineering, KSRM College of Engineering , Kadapa, mesrinu@rediffmail.com.

***Abstract*- Ad-hoc Wireless Sensor Networks usage spreading rapidly due to their flexibility to provide communication in unattended and hostile environment like military target tracking and weather prediction, without fixed infrastructure to provide communication. In Ad-hoc Wireless Sensor Networks nodes are communicate while moving. Since lack of physical security, it easily prone to security attacks. The network suffers from various attacks such as wormhole, black hole, and selective forwarding attack. Selective forwarding attack is a severe threat enables a compromised node behaves like normal node and may drops packets selectively. It deteriorates the performance of networks and integrity of information. Due to resource limitations of sensor nodes, it is not feasible to use conventional security solutions, which requires complex computations and more memory. Due to nodes mobility, it is a challenging task to detect selective forwarding attacks in Ad-hoc Wireless Sensor Networks. In this paper, we discuss some of the authentication strategies and detection techniques to defend and defeat against selective forwarding attacks.**

***Keywords* - Ad-hoc Wireless Sensor Network, Selective Forwarding Attacks, Authentication.**

I.INTRODUCTION

Ad-hoc Wireless Sensor Networks are developed as promising technology. Ad-hoc Wireless Sensor Networks is collection of peer mobile sensor nodes, which are capable of communicating with each other without any fixed infrastructure. In this Nodes are self-organized and self-configured. It is used in real-time applications for continuous monitoring, gathering, process, analysis, and transmission of data in hostile environment. Ad-hoc networks are easy to deploy and used in application, where infrastructure is not available, destroyed or not possible. It is mainly used in monitoring applications. Some of the prevalent applications are military-battle field, healthcare, disaster and relief, transportation, construction, agriculture, business, wild life monitoring, area monitoring, environmental monitoring, machine health monitoring, vehicular movement and nuclear power plant. Sensor node consists of elements like sensor, battery, memory, microcontroller, and radio transceiver. In Ad-hoc WSN two types of sensor nodes are available, generic sensor nodes and Gateway node.

Because of limited transmission capacity of sensor node, there is no end-to-end transmission. The sensor node use multi-hop transmission and transmit packets with co-operation of intermediate nodes to the base station. The topology of Ad-hoc networks changes rapidly due to node mobility, joining, or failure. Adversary can easily compromise a sensor node along the transmission path from source node to base station, due to lack of physical protection of nodes. A Compromised node can alters data, eavesdrop on packets and inject fake packets. Vulnerable security attacks in WSN are

Black hole Attack: A Malicious Node can drop all packets transmit through it.

Worm hole Attack: Transmit packets from region to another region in WSN.

Sink hole Attack: Adversary can receive packets from all the nodes in WSN.

Sybil Attack: Malicious node has multiple identities in WSN.

Node Replication: Malicious node could impersonate an existing node.

Acknowledgment Spoofing: An illegitimate node could imitate acknowledgement to announce weak path as strong path.

Hello Packet Flooding: An Adversary node generates Hello Packet with high energy level, to ensure that all nodes misunderstand that it is sink node.

Selective Forward Attack: A compromised node can drop packets selectively.

In Ad-hoc WSN attacks are mainly considered from two different perspectives 1) Attacks against security 2) Attacks against Routing. In WSN attackers are mainly classified into two types 1) Inside attacker 2) Outside attacker. Authentication schemes are used to prevent outside attackers from enters into WSN. Intrusion Detection Schemes are used to detect and defend against inside attacker. So we use authentication schemes as first level and detection schemes as second level to provide attack-avoid data forwarding in ad-hoc WSN.

In this paper we present an overview regarding authentication schemes and detection techniques to prevent selective forwarding attacks in Ad-hoc WSN developed by earlier researchers in the domain of WSN. The next sections of this paper are described as follows. In Section-II, presented selective forwarding attacks and its classification. In section-III, described authentications strategies to defend against selective forwarding attacks. In section-IV , discussed detect and defeat techniques of selective forwarding attacks. In section-V, conclude the survey on selective forward attacks in ad-hoc WSN.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

II.SELECTIVE FORWARDING ATTACKS

Selective Forwarding Attack is one of the network layer attacks in Wireless Sensor Networks first proposed by Karlof [1]. It can corrupt a number of existing routing protocols such as Tinos beaconing, Directed diffusion, GPSR [1]. In selective forwarding attack a malicious internal node may drop or forward some of the packets transmitted through it. It is more dangerous when the attacker present on the path of data transmission. Selective forwarding attacks show negative impact in data–sensitive applications like military-battle field, Environment monitoring etc. In Ad-hoc WSN packets are lost due to noise fluctuations in wireless radio transmission and medium access collision. The Selective forwarding attacks are hidden by normal packet loss. The detection of attacks in the network is difficult; it needs to determine whether the packets are lost due to either attacks or disturbance in transmission radio or any other reason. It makes the task of attack detection is a complex and challenging task.

Selective Forwarding Attacks are classified in view of the packets drop as 1) drop packets of specified node 2) drop packets of specified type [2].`Selective Forwarding Attacks also categorized in view of node count in multi-hop network as a) single malicious node b) two consecutive malicious nodes c) surrounding malicious nodes d) non-consecutive malicious node are shown in Fig.1. [1].

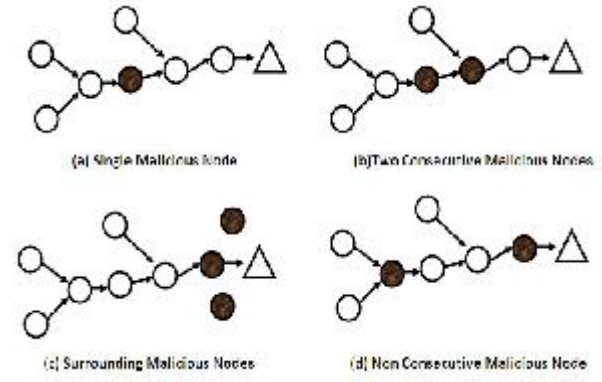

Fig. 1. [1] Types of Selective Forwarding Attacks based on node count

Different forms of selective forwarding attacks based on nature of forwarding as 1) drops some packets 2) forward some packets to the wrong path 3) delays packet transmission through network creates confused routing between sensor nodes [3]. To secure wireless sensor networks, it has to satisfy all the security properties like Integrity, Confidentiality, availability and authenticity. Counter measures of selective forwarding attacks in Ad-hoc Wireless Sensor Networks are broadly classified into two types based on nature of schemes.

1. Authentication Strategies/Protocols: These are used to prevent selective forwarding attacks occurrence in WSN by prevent the attacker from compromises a legitimate node in network.
2. Detection and Remove Techniques: These are used to detect the occurrence of selective forwarding attacks and remove the malicious node from packet routing. Detection Techniques again classified into two types based on the information used to detect the attack and malicious node.
   a. Acknowledgement based detection: In this attack and malicious node are detected using acknowledgements received from nodes along the transmission path from source to destination.
   b. Detection based on neighborhood information: In this attack and malicious node are detected using the information received from neighbor nodes about forwarding behavior of node.

III.AUTHENTICATION STRATEGIES

It is advantageous to prevent adversary instead of detect a malicious node in large scale and Real-time Ad-hoc Wireless Sensor Networks. Authentication is used to prevent the unauthorized users from access the sensor nodes in the network. The authentication protocol developed using conventional cryptography can consume more resources and leads to denial of service [14]. The Wireless sensor Networks can use public key cryptography for node or user authentication and, key agreement for current session between sensor node, user and vice-versa. The task of providing authentication consider the aspects like design an authentication protocol, formal analysis of protocol, implementation of protocol using security tools, and evaluate the quality of protection provided by the protocol [14]. The challenges in designing an authentication protocol are minimize computation and communication cost and maximizes the protection from adversary, deals adding a new node and node failure dynamically. Ad-hoc WSN demands real-time routing where the message to be delivered within constrained time.

A. Security with Pre-loaded Time Limited Memory Keys(TMLK)

Described [20] security scheme based on Time Limited Memory Key (TMLK). It is a Symmetric key Protocol. In this the key is saved in the RAM of device, so that it is hard to read RAM of the running program from outside. Program reset will automatically erase the contents of RAM. Along with the symmetric key,its lifetime also transferred to the target node from key distribution center (KDC).The protocol have three phases.

Key pre-deployment: Each node has unique ID and get initial key from KDC. It must be done in secure Environment that ensures no one can listen the communication. Also re-flash the nodes software to be sure that no nodes are operating with other algorithms. Authentication is not necessary because each node gets secret key from trusted KDC.

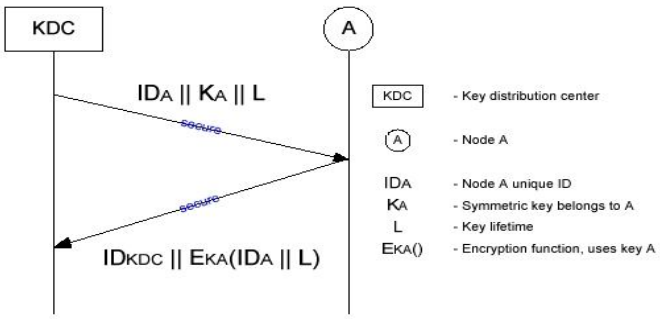

Fig. 2 [20] Key Pre-deployment

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Key update/revoke: To keep node inside the network, the node's symmetric key must be updated regularly within interval smaller than key's life time 'L'. The revocation of the node is fairly not to update the node's key after time 'L'. The node will automatically remove.

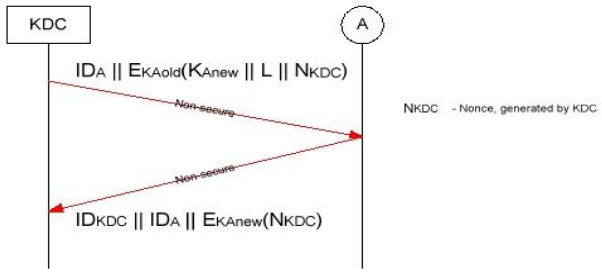

Fig. 3 [20] **Key** Update

Message Exchange: To exchange data in a secure manner between nodes we use transparent symmetric message encryption through KDC. It provides mutual authentication and message delivery acknowledgement. Because of symmetrical nature both nodes have perform same amount of computations.

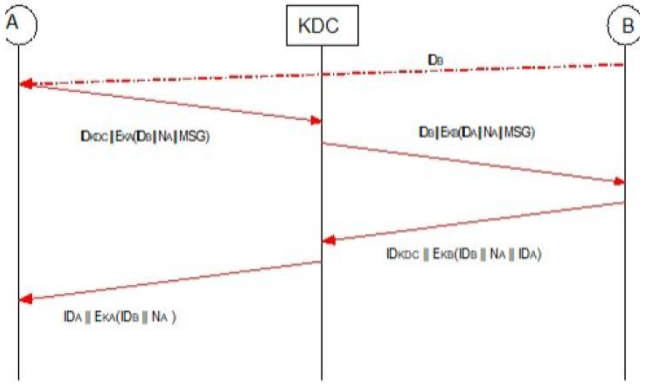

Fig.4.[20] Transparent message encryption

Benefits of the Protocol are keys are secure and provide mutual authentication, Easy to identify Intruder in the network.

Limitations of the protocol are A compromised KDC will compromise all the network. If KDC is blocked from all nodes for time period greater than key life time 'L', then entire network will be destroyed. Not suitable for large sized networks because groups can only be made based on trusted KDC, that must provide trusted communication.

B. Biometric Authentication Protocol

Presented [21] a user authentication protocol based on biometric (users iris). This protocol involves light weight hash and EX-OR operations. In this protocol iris of the user is users to reproduce the user's key whenever the user wants to access the nodes in the network. It enhances the security because iris is the unique trait of each user. The authentication protocol uses encryption and hash functions with less computation cost. The key (iris) used is stronger than password and shorter than Biometric data. The protocol has four phases 1.Registration 2.Login 3.Authentication 4.User's key change. The protocol states the given assumptions.

1. The Gate Way Node (GWN) is treated as trusted node.
2. Each user musr register with the system to access WSN.

Registration Phase: Whenever the user $U_i$registers, an encrypted key will be generated for U_i and it is saved on GWN. After that the U_i iris are extracted and hashed, then EX-ORed with the key to generate BE template, which will be saved in user device will be used for regenerate key from user's iris for authentication. The hash value of the key will be saved with the BE template as shown in below figure.

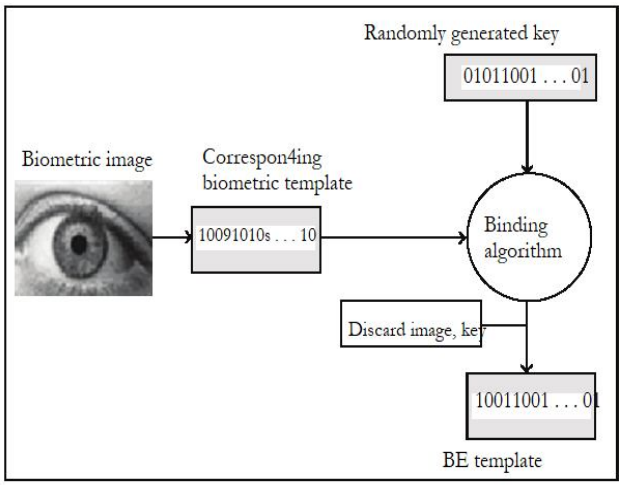

Fig.5.[21] Biometric cryptography

Login Phase: In this first extract the user's iris and hashed, and EX-ORed with BE template to reproduce the user's key. Then the newly generated user's key is hashed and compared with saved hash value of user's key. If two hash values are not equal the authentication is aborted, otherwise sent a login request to GWN with user's ID_i.

Authentication Phase: When GWN receives a login request from user, it respond with a random nonce R. When the user receives random nonce from GWN, it will send sent the encrypted message of R and current time stamp T1 to GWN using the encryption key. Then GWN receives encrypted message , decrypt it using the corresponding user's key at time stamp T2 and abort the authentication if |T2-T1| is greater than normal transmission delay. Otherwise continue the authentication process.

1. The GWN computes Fi = h(ID$i\oplus X$), and Yi = MACF(IDi ‖SN‖$T3$) where SN is the sensor node which will reply to the user's query. The GWN transmits a message (IDi, Yi, $T3$) to SN.
2. When SN receives message from GWN , SN computes Fi = h(ID$i\oplus X$) and Y^*i = MACF(IDi ‖SN‖$T3$), Verify Y^*i = Yi, if yes SN respond to the user's query RM and compute Vi = h(IDi ‖Fi ‖$T5$) and Ci = h(RM).Then compute L = $E\_$(RM, Ci) and send a message (L, $T5$) to user.
3. when the user receives the massage (L, $T5$) computes Vi = h(IDi ‖Fi ‖$T5$) and decrypt the message L with $V_i$to get RM and Ci {RM, Ci}= $D_{Vi}(L)$ and compute Ci^* = h(RM)Verify Ci^* = Ci, if yes accept RM.

User Ui GW node Sensor Node(SN)

Select sensor login-node SN

Pick up timestamp $T3$

Fi = h(ID$i\oplus X$)

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Yi = MAC(IDi || SN || $T3$)

(IDi, Yi, $T3$) →

Verify ($T4 - T3$) $\leq \Delta T$

$Fi = h$(ID$i \oplus X$)

Y^*i = MAC(IDi || SN || $T3$)

Verify $Y^*i = Yi$?

RM = respond to the Ui query

Pick up timestamp $T5$

$Vi = h$(IDi || Fi || $T5$)

$Ci = h$(RM)

$L = E\_$(RM, Ci)

← (L, $T5$)

Verify ($T6 - T5$) $\leq \Delta T$

$Vi = h$(IDi || Fi || $T5$)

{RM, Ci}= $D\_i(L)$

$C^*i = h$(RM)

Verify $C^*i = Ci$?

Accept RM

Fig.6.[21]: Authentication phase

Key Change Phase: The user's key can be changed by re-enrollment process using users biometric, when the key is compromised a new key is generated randomly which is different from previous one.

The merits of the protocol are, It provides user authentication without transmitting and storing any private information. It is more reliable than conventional password based authentication. It is efficient and light weight in terms of computation and communication. The demerits of the protocol are, There is no authentication of sensor node at user before accept the response to verify whether it is send from a legitimate sensor node or not. There is a possibility of session specific information attack, Adversary can compromise user device and extract the information stored in the user device <IDi, Fi> and try to eavesdrop the message RM from Sensor Node to user by compute decryption key Vi=h(IDi||Fi||T5) and decrypt message L using Vi as (RM, Ci)=Dvi(L). It also requires extra H/w.

C. Password based User Authentication Protocol

Described [22] an authentication and key agreement protocol for ad hoc wireless sensor networks. It is based on dynamic password, which is changed in each session of communication. The Protocol has five phases. The following notations are used in the protocol description.

U_i	The user
ID_i	The identity of U_i
PW_i	The password of U_i
SC_i	The smart card of U_i
GWN	The gateway node
S_j	The sensor node
SID_j	The identity of S_j
X_{GWN}	The long-term secret of GWN
X_{GWN-U_i}	The secret shared between GWN and U_i
X_{GWN-S_j}	The secret shared between GWN and S_j
T_1, T_2, T_3, T_4	The timestamps
ΔT	The expected transmission delay
$r_i, r_i', r_j, K_i, K_j, a, b$	The random numbers
P	A point on the elliptic curve
Px	The x-axis value of the point P
$\|, \oplus, h()$	The concatenation, XOR, and hash operation

Table 1[22] : Notations

Pre-deployment Phase: Each sensor node Sj is assigned an identity SIDjand a randomly-generated secret XGWN−Sj . The GWN stores SIDj and XGWN−Sj in its memory.

Registration Phase: The users and sensornodes register with the gateway node GWN. The registration of a user Ui consists of the following steps:

1. The user Ui selects an identity IDi and a passwordPWi , and chooses a random number ri . Ui computesMPi = h(ri||PWi), MIi = h(ri||IDi), and sends themessage mUreg = {MIi , MPi } to GWN via a secure channel.

2.GWN chooses a secret XGWN−Ui for Ui , then storesMIi and XGWN−Ui into its memory. It computesfi = h(MIi||XGWN), xi = h(MPi||XGWN−Ui),ei = fi ⊕ xi , and issues the smart card SCicontaining {MIi , ei , fi , XGWN−Ui} to Ui .

3. Ui writes ri into SCi .

The registration of a sensor node Sj is described as follows.

1. Sj selects a random nonce rj , and computes MPj =h(XGWN−Sj||r j||SIDj), MNj = rj ⊕ XGWN−Sj ,RMPj = MPj ⊕ MNj , then sends mSreg1 ={SIDj , MNj , RMPj , T1} to GWN via an unsecurechannel.

2 If T1 is valid, GWN computes MPj = RMPj ⊕MNj , r j*= MNj ⊕ XGWN−Sj , and MPj*=h(XGWN−Sj||r j||SIDj). If MPj*= MPj ,GWN computes f j = h(SIDj||XGWN), x j =h(MPj*||XGWN−Sj), e j = f j ⊕ x j , and sendsmSreg2 = {e j , f j , T2} to Sj .

3. If T2 is valid, Sj has succeeded in registering toGWN. Finally, it stores e j and f j into its memory.

Login Phase: In this phase, Ui choose the sensor nodeSj to which it wants to communicate with and performs the loginas follows.

Ui inputs the password PWi* . SCicomputes MPi*= h(ri||PWi*), xi*= h(MPi*||XGWN−Ui). IfXi*= xi , SCi selects a random nonce Ki , and computes Ni =h(xi||XGWN−U||T1), Zi = Ki ⊕ fi . Then, it sends the loginrequest m1 = {MIi , ei , Zi , Ni , T1} to Sj .

Authentication Phase: After receiving the login message m1 from Ui , the sensor node Sj authenticates Ui as given below

1. If T1 is valid, Sj computes xj=ej⊕fj,Aj=h(XGWN−Sj||T1||T2) ⊕ x j , and sends m2 ={MIi , ei , Ni , T1, T2, SIDj , e j , Aj } to GWN.

2. GWN verifies T1 and retrieve the secret XGWN−Sj corresponding to SIDj in its memory. It computes fj*=h(SIDj||XGWN),xj*=ej⊕fj*,xj=Aj⊕h(XGWN−Sj|T1||T2). If xj*= xj, GWN has successfullyauthenticated Sj ; otherwise, it terminates thesession.

GWN computes f i*= h(MIi||XGWN),xi*= ei ⊕ fi* , and Qi = h(xi*||XGWN−Ui||T1). If Qi = Ni , Ui is authentic.

GWN computes Hj = h(fj*||XGWN−Sj||T1||T2||T3), Fij = f i*⊕ h(fj*||XGWN−Sj), Ei = h(Qi ||T1||T2||T3), and sends m3 = {Fij , Hj , Ei , T1, T2, T3}to Sj .

3. If T3 is valid and Hj* = h(f j||XGWN−Sj||T1||T2||T3), if Hj*=Hj ,Sj has successfully authenticated both GWN and Ui , and it selects a random nonce K j . Then, it computes f i*= Fi j ⊕ h(f j||XGWN−Sj), Ki*= Zi ⊕ fi* , Ri j = h(fi*||SIDj ||T1||T2||T3||T4) ⊕ K j , the sessionkey SK = h(Ki ⊕ K j), and sends the messagem4 ={Ei , Ri j , T1, T2, T3, T4} to Ui .

4. If T4 is valid and Ei = h(Ni||T1||T2||T3), Ui truststhat Sj isgenuine.Then computes Kj=Rij⊕h(fi||SIDj||T1||T2||T3||T4) and the session key SK= h(Ki ⊕ K j).

Password-change Phase: *Ui* inputs the current password PWi^{OLD}. *SCi* computes *MPi**= h(ri||PWi^{OLD} *i)* and*xi**= fi* ⊕*ei*. If *xi**= xi* , *Ui* inputs the new password PWi^{NEW}. *SCi* computes *MPi***= h(ri||PWi^{NEW}*)*, xi^{NEW}=*h(MPi***||*XGWN−Ui *)*, and ei^{NEW}= *fi*⊕xi^{NEW}. Finally, *SCi*replaces the old value *ei* with the new value ei^{NEW}in itsMemory.

Flaws in Turkanovic et al.'s Protocol are

ISSN:0971-1260
Vol-22- Issue-14-December-2019

*If A*n adversary obtains a smart card of a legitimate user, then it uses the information stored in the smart card's memory to gain access to any sensor node.

An adversary masquerades as a legitimate user and gains access to one or many sensor nodes simultaneously after compromising one of them.

After compromising one sensor node, an adversary can masquerade as any legitimate sensor node to which a user is trying to log in.

*The*session key is computed as $SK = K_i \oplus K_j$, where $K_i = Z_i \oplus f_i$ and $K_j = R_{ij} \oplus h(f_i||SID_j||T_1||T_2||T_3||T_4)$. Therefore, if an adversary could obtain f_i, it cancompute the session key SK between U_i and any sensor nodesince Z_i and R_{ij} are transmitted over unsecure channel. The adversary can always acquire f_i. Therefore, the scheme failsto provide both forward and backward secrecy.

D. Secure and Efficient Authentication Protocol for Ad hoc WSN

Presented [23] a secure, efficient and flexible authentication protocol using ECC (Elliptic Curve Cryptography) for ad hoc Wireless Sensor Networks. There are two ways to authenticate user in WSN. One is, the user is authenticated by Gate Way Node before communicate with sensor node. The second is user directly contacts sensor node and perform authentication with it. In this protocol 1) user initially sends a login request to sensor node 2) sensor node forwards the user's login request to GWN for authentication. 3) When sensor node receives a positive response from GWN accepts user and 4) replies with key establishment information. This protocol is use to solve the weaknesses in Turkanovic [22] authentication protocol and provide secure authentication by using ECC for key agreement between sensor node and user. This protocol provides forward secrecy. This protocol does not need to store any secrete information regarding users and sensor nodes.

Elliptic Curve Cryptography (ECC) denote the group of points of the elliptic curve $Ea,b : y^2 = x^3 + ax + b$ overthe finite field Fq, where $a, b \in Fq$ satisfy $4a^3 + 27b^2 != 0 \bmod q$. Where q is large prime. Let $Gp = (P)$be a cyclic group of prime order p,where P is a generator point of the group and $P \in Ea,b(Fq)$. The three mathematical problems [20] in Elliptic CurveCryptography (ECC) are defined as follows:

• The *discrete logarithm* (ECDL) problem is to find a based on given point$Q \in Gp$, where $a \in Zp$ and $Q = aP$.

• The *computational Diffie-Hellman* (ECCDH) problem is to find abP for the given aP and bP, where $a, b \in Zp$.

•The *decisional Diffie-Hellman* (ECDDH) problem is to decide whether $abP = cP$ when given aP, bP and cP, where $a, b, c \in Zp$.

The protocol has four phases: 1) pre-deployment phase, 2) registration phase, 3) authentication phase, and 4) password changing phase.

Pre- deployment phase: In this the gateway node *GWN* is assigned a randomly generated long-term secret *XGWN*. Each sensor node *Sj* , has assigned an identity *SIDj* , the GWN computes $f_j = h(SID_j||XGWN)$, and the information *SIDj* and f_j are written into the memory of sensor before deploying *Sj* into the network.

Registration Phase*:* In this phase a user U_i registers with the gateway node before access to the sensor nodes in a wireless sensor network.

1. U_i choose an identity *IDi* , a password *PWi* , and generates a random number *ri* . Then computes $MP_i = h(r_i||PW_i)$ and sends message $mUreg = \{ID_i, MP_i\}$ to *GWN*.
2. When GWN receives *mUreg*, it verifies the user's identity and generates a random number *ri*. Next, *GWN* computes the pseudo-identity$MI_i = h(r_i||ID_i)$ for U_i , and uses its long-term secret *XGWN* to compute $f_i = h(MI_i||XGWN)$, and $e_i = MP_i \oplus f_i$. Lastly, *GWN* personalises a smart card *SCi* containing $\{MI_i, e_i\}$ sends it to U_i .
3. After receipt of the smart card *SCi* , the user U_i writes the value r_i into it. Finally, the smart card contains $\{MI_i, e_i, r_i\}$.

Authentication Phase*: Used to authenticate the user, w*hen a user U_i wants to log into a sensor node S_j. The user U_i follow the given steps

1. The user U_i inserts the smart card *SCi* into a terminal, and inputs the identity ID_i and the password PW_i .

The smart card computes $MP_i = h(r_i||PW_i)$, $f_i = e_i \oplus MP_i$ and $Y_i = h(f_i||T_1)$, where T_1 is current timestamp of SC_i. Next, SC_i chooses a random number *a belongs to*Z_p and computes $K_i = aP$.Then computes $Z_i = K_i \oplus Y_i$, and $N_i = (Y_i||MI_i||SID_j)$. After that, sends the login request $m1 = \{MI_i, Z_i, N_i, T1\}$ to the sensor node S_j .

2. After receiving $m1$ from U_i , the sensor node S_j verifies the timestamp $T1$. If $T1$ is valid, S_j takes the current timestamp $T2$ and computes $A_j = h(f_j||N_i||T2)$, where f_j is in the node's memory; Then the sensor node sends the message $m2 = \{MI_i, N_i, SID_j, A_j, T1, T2\}$ to the gateway node *GWN*.
3. Upon receipt of $m2$ from S_j , the gateway node verifies both $T1$ and $T2$. If both $T1$ and $T2$ are valid, the GWN uses its long-term secret *XGWN* to compute $f_j' = h(SID_j||XGWN)$, $f_i = h(MI_i||XGWN)$, $A'_j = (f'_j||N_i||T2)$, $Y'_i = h(f'_i||T1)$, and $N'_i = h(Y'_i||MI_i||SID_j)$. After that, *GWN* verifies A_j and N_i in $m2$. If $N'_i = N_i$ and $A'_j = A_j$, the gateway accepts U_i ; otherwise, it rejects U_i . After successfully authenticating U_i , *GWN* computes $F_{ij} = Y'_i \oplus h(f'_j||T3)$, $H_j = h(Y'_i)$, and $E_i = h(f'_i||N'_i)$ and sends $m3 = \{F_{ij}, H_j, E_i, T3\}$ to S_j .
4. After receiving $m3$, the sensor node S_j verifies $T3$. If $T3$ is valid, S_j computes $Y'_i = F_{ij} \oplus h(f_j||T3)$ and $H'_j = h(Y'_i)$. If $H'_j = H_j$, then sensor node accepts U_i ; otherwise, it rejects U_i . Then,it selects a random number b*belongs to* Zp and computes $K_j = bP$ *an*d computes $K'_i = Z_i \oplus Y'_i$, $R_{ij} = h(K'_i||T4) \oplus K_j$, whereby $T4$ is the current timestamp. After that sending the message $m4 = \{R_{ij}, E_i, T4\}$ to U_i , then sensor node computes the session key $SK = h(bK'_i.x) = h(abP.x)$, where $abP.x$ is the x-coordinate of the point abP.
5. After receiving the reply message $m4$ from S_j, the smart card *SCi* tests $T4$. If $T4$ is valid, SCi computes$E'_i = h(f_i||N_i)$ and verify whether $E'_i = E_i$. If yes,S_j is authenticated and computes $K'_j = R_{ij} \oplus h(K_i||T4)$. Then,$SC_i$ calculates the

ISSN:0971-1260
Vol-22- Issue-14-December-2019

session key $SK = h(aK'j.x)=h(abP.x)$, where $abP.x$ is the x-coordinate of the point abP.

The SCi and Sj exchange data successfully over the secure channel using valid session key SK.

Password Changing Phase: Assumes that the user Ui is authenticated earlier. When user wants to change password, Ui inserts the smart card into a terminal and enters the identity $I\ Di$ and the password PWi . Then smart card calculates $MPi = h(ri \| PWi)$ and requests Ui to input a new password PW_i^{new}. Then, SCi computes $MP_i^{new}=h(ri \| PW_i^{new})$ and $e_i^{new}=ei \oplus MPi \oplus MP_i^{new}$. Finally, replaces ei by $e_i^{new}i$ in smart card memory.

Security Vulnerabilities in Chang et al.'s Protocol

1. User's ID_i and PW_i are verified at GWN in step 3 of authentication phase. But it is common for a user to forgot or enter a incorrect password and sensor node also send incorrect credentials to the GWN. Then GWN verify authentication and finds that incorrect credentials. So, it leads to waste of GWN processing time and unnecessary consumption of sensor node's energy.
2. When the user tries to login with incorrect ID and correct PW, he is authenticated by GWN. So, the protocol does not verify the ID of the user.
3. An adversary can able to guess user's password by extract all the stored information into the user's smart card by conduct online/offline password guessing attack.
4. An adversary can able to trace the user by compare two messages send by user in two different sessions based on comparing MI of the user. So, the protocol has user traceability attack.

E. Untraceable and Anonymous Password Authentication Protocol

Proposed [25] a reliable authentication protocol for ad hoc wireless sensor networks to defend against active and passive attacks. The solution to defend against attacks in the network is user authentication and session key agreement. A sensor node consumes more power to transmit a message than to receive a message. So, it consumes more power to transmit a message over a long distance 26]. In this protocol a user access data from the sensor node through Gate-Way-Node. Since sensor node communicates with nearest GWN, it reduces the power consumption for communication. This protocol has eight phases. It is used to reduce the vulnerable attacks in C.C.Chang's protocol [23]. The notations used in this protocol are described in given table.

Notations	Description
Ui	**i-th User**
SCi	Smartcard of Ui
S j	Sensor node
GWN	Gateway node
Z*q	multiplicative group, where q is a large, prime number Z*q = fx : 0 < x < q; gcd(x, q) = 1
PWi	Password of Ui
IDi	Identity of Ui
Bi	Biometric of Ui
S IDj	Identity of S j
XGWN	Secret key of the GWN
f j	Secret key of the S j
Ki	Random number generated by Ui
Kj	Random number generated by S j
Ti	Timestamp
ΔT	Allowable transmission delay
SKi;gwn; j	Session key
h(.)	Cryptographic One-way hash function
REP(.), GEN(.)	Fuzzy extractor operation
‖	Concatenation operation
⊕	Bitwise XOR operation

Table 2[25] : Notations

Pre-deploymentphase: In this the gateway node *GWN* is assigned a randomly generated long-term secret *XGWN*. Each sensor node *Sj* , has assigned an identity *SIDj* , the GWN computes $f j = h(SIDj \| XGWN)$, and the information *SIDj* and $f j$ are written into the memory of sensor before deploying *Sj* into the network.

User RegistrationPhase: In this phase user $U_i$submits login credential to *GWN*, then it verifies the credentials and issues a smart- card to U_i. It comprises of following steps.

1. Ui selects an identity IDi and sends this along with a unique credential (e.g., voter identity card or social security number) to GWN through a secure channel .
2. GWN verifies for IDi in the database. If IDi available in the database, then GWN prompts Ui for another identity;otherwise, GWN calculates MIi = h(IDi ||ri) and fi = h(MIi ||XGWN), GWN delivers a new smartcard SCi to Ui via a secure channel after writing (MIi; fi) into SCi.

3. When receiving SC_i, $U_i$keys ID_i, PW_iin $SC_i$and biometric information $B_i$at the sensor device. Note that thispaperusesthefuzzyextractortechnique[27]forthebiometric enrollment.SC_icomputes$(\psi_i,\theta_i) = GEN(B_i)$, $A_i=h(ID_i \| PW_i \| \psi_i), E_i=\theta_i \oplus h(ID_i \| PW_i), C_i=f_i \oplus h(PW_i \| \psi_i), REC= PW_i \oplus h(ID_i \| \psi_i), REG_i=h(ID_i \oplus \psi_i)$ andwrites$(C_i,E_i,A_i,REC,REG_i,GEN(),REP(),h())$into$SC_i$and deletes$f_i$.$SC_i$alsowrites$(REC,REG_i)$.Finally, SC_iencloses$(MI_i,C_i,E_i,A_i,REC,REG_i,GEN(),REP(),h())$.

LoginPhase: When user $U_i$wants to access data from sensor S_j, U_i*performs* the following steps:

1.$U_i$insertsSC_iintotheterminalandinputs(ID_i^J, PW_i^J)andB_i^Jatthesensordevice.SC_iretrieves$\theta_i = E_i \oplus h(ID_i^J \| PW_i^J)$andcalculates$psi_i^J = REP(B_i^J,\theta_i), f_i=C_i \oplus h(PW_i^J \| \psi_i), A_i^*=h(ID_i^J \| PW_i^J \| \psi_i)$.Now,$SC_i$verifies$A_i^*?=A_i$.If$(A_i^* != A_i)$,then$SC_i$rejects$U_i$;otherwise,itimplies$ID_i^J=ID_i, PW_i^J=PW_i$ and$B_i^J=B_i$.

2.SC_iproduces$K_i \in_R Z_q^*$andcalculates$N_i=h(MI_i \| K_i \| f_i \| T_1 \| SID_j), L_i = K_i \oplus h(MI_i \| f_i \| T_1), P_i = SID_j \oplus h(f_i \| T_1), Q_i=h(ID_i) \oplus h(K_i \| T_1)$, where T_1 is the current timestamp.

3.Lastly SC_isends $(MI_i, N_i, P_i, Q_i, L_i, T_1)$ to *GWN*.**Authentication and Session Key AgreementPhase:** This phase used to establish session key between Ui and S j throughGWN,

1.Whenreceiving$(MI_i,N_i,P_i,Q_i,L_i,T_1)$,*GWN*verifieswhetherthe timestampcondition$|T_1-T_2| \le \Delta T$holds. Ifitdoesnothold,then*GWN*believes$(MI_i,N_i,P_i,Q_i,L_i,T_1)$isincorrect.Otherwise,*GWN*calculates$f_i^J=h(MI_i \|$

ISSN:0971-1260
Vol-22- Issue-14-December-2019

X_{GWN}), $K_i^J = L_i \oplus h(MI_i \| f_i^J \| T_1)$, $h(ID_i) = Q_i \oplus h(K_i^J \| T_1)$, $SID_j^J = P_i \oplus h(f_i^J \| T_1)$, $N_i^J = h(MI_i \| K_i^J \| f_i^J \| T_1 \| SID_j^J)$. Then, *GWN* checks whether $N_i^J ?= N_i$ holds. If ($N_i^J = N_i$), then *GWN* believes that $MI_i, N_i, P_i, Q_i, L_i, T_1$ is generated by an authorized; otherwise, *GWN* terminates the connection.

2. *GWN* computes $f_j^J = h(SID_j^J \| X_{GWN})$, $N_j = h(h(ID_i) \| f_j \| T_2 \| K_i)$, $SS_j = h(ID_i) \oplus h(f_j^J \| T_2)$, $V_j = K_i \oplus h(ID_i)$ and sends (N_j, SS_j, V_j, T_2) to S_j through an open channel.

3. After receiving (N_j, SS_j, V_j, T_2), S_j checks whether $|T_2 - T_3| \le \Delta T$ holds. If it is false, then S_j terminates the connection; otherwise, S_j computes $h(ID_i) = SS_j \oplus h(f_j \| T_2)$, $K_i^J = V_j \oplus h(ID_i)$, $N_j^J = h(h(ID_i) \| f_j \| T_2 \| K_i^J)$. S_j then verifies whether $N_j^J ?= N_j$ holds. If it is incorrect, then S_j discontinues the session; otherwise, S_j produces $K_j \in_R Z_q^*$ and calculates $SK_j = h(h(ID_i) \| SID_j \| K_i^J \| K_j)$, $W_j = h(SK_j \| T_3)$, $K_{ij} = K_i \oplus K_j$. Finally, S_j sends (W_j, K_{ij}, T_3) to *GWN* using an open channel.

4. After receiving (W_j, K_{ij}, T_3), *GWN* verifies if $|T_3 - T_4| \le \Delta T$ holds. If it is false, then *GWN* discontinues the session; otherwise, *GWN* computes $K_j^J = K_{ij} \oplus K_i$, $SK_{GWN} = h(h(ID_i) \| SID_j^J \| K_i^J \| K_j^J)$, $W_j^J = h(SK_{GWN} \| T_3)$ and verifies whether $W_j^J ?= W_j$ holds. If it incorrect, then *GWN* aborts the session; otherwise, *GWN* calculates $M_1 = h(SK_{GWN} \| K_j^J \| T_4)$ and sends (M_1, K_{ij}, T_4) to U_i through a public channel.

5. After receiving (M_1, K_{ij}, T_4), U_i checks whether $|T_4 - T_5| \le \Delta T$ holds. If it is false, then U_i terminates the session; otherwise, U_i calculates $K_j^J = K_{ij} \oplus K_i^J$, $SK_i = h(h(ID_i) \| SID_j \| K_i \| K_j^J)$, $M_1^J = h(SK_i \| K_j^J \| T_4)$ and also verifies whether $M_1^J ?= M_1$ holds. If it is true, then the protocol completes both mutual authentication and session key negotiation between the entities involved.

6. In order to achieve user untraceability, U_i delivers a confirmation message to *GWN* along with M_2, where $M_2 = ID_i \oplus h(SK_i \| K_i)$. Then, *GWN* extracts $ID_i^J = M_2 \oplus h(SK_{GWN} \| K_i)$ and calculates $MI_i^J = h(ID_i \| r_i^J)$, $f_i^J = h(MI_i^J \| X_{GWN})$, $M_3 = MI_i^J \oplus h(ID_i)$, $M_4 = f_i^J \oplus h(f_i \| K_i)$, $M_5 = h(h(ID_i) \| M_3 \| M_4)$. *GWN* now transmits ($M_3, M_4, M_5$) to U_i through an insecure/open channel, where $r_i^J \in_R Z_q^*$ and $r_i^J != r_i$.

7. After receiving (M_3, M_4, M_5), U_i calculates $M_5^J = h(h(ID_i) \| M_3 \| M_4)$ and verifies $M_5^J ?= M_5$. If ($M_5^J = M_5$, then U_i considers that the message received from *GWN* is correct. U_i extracts $MI_i^J = M_3 \oplus h(ID_i)$, $f_i^J = M_4 \oplus h(f_i \| K_i)$, $C_i = f_i^J \oplus h(ID_i \| \psi_i)$. Finally, U_i writes (MI_i^J, C^i) and deletes the previous MI_i and C_{ij} values from the memory

Post-Deployment Phase:
This phase used to replace a damaged sensor node S_j with a new sensor node S_k. *GWN* chooses the identity SID_k of S_k and then calculates $f_k = h(SID_k \| X_{GWN})$. *GWN* stores SID_k, f_k in the memory of S_k prior to field deployment.

Password Recovery Phase:
If U_i forget the password, then U_i executes this phase. U_i inserts SC_i and provides ID_i along with B_i at the sensor device. SC_i then computes $psi_i^J = REP(B_i^J, \theta_i)$ and $REG_i^J = h(ID_i \oplus psi_i)$. SC_i checks whether $REG_i^J ?= REG_i$ holds. If ($REG_i^J = REG_i$), then SC_i calculates $PW_i = REC \oplus h(ID_i \| \psi_i)$ and sends PW_i to U_i

Password Change Phase:
To provide more security, the organizations need to change the password regularly. So, this phase is used periodically to change the password. This phase is as follows:

1.
U_i inserts SC_i into the terminal and enters (ID_i^J, PW_i^J) along with bio metric information B_i^J. SC_i extracts $\theta_i^J = E_i \oplus h(ID_i^J \| PW_i^J)$ and finds $psi_i^J = REP(B_i^J, \theta_i^J)$, $f_i = C_i \oplus h(PW_i^J \| \psi_i^J)$, $A_i^* = h(ID_i^J \| PW_i^J \| \psi_i^J)$. If ($A_i^* != A_i$), then SC_i aborts this phase; otherwise, SC_i requests U_i to enter a new password. Thus, U_i enters a new password PW^{new}_i != PW_i at SCi

Smartcard Revocation Phase: It is when smartcards can be misplaced, stolen or damaged.

1. Ui provides IDi along with personal credential information to the smartcard issuer. Based on the received information, the issuer verifies whether the supplied information is valid. If yes, then the issuer calculates $MI^{new}_i = h(ID_i \| r_i)$, $f^{new}_i = h(MI^{new}_i \| X_{GWN})$, writes ($MI^{new}_i, f^{new}_i$) into a new smartcard SC^{new}_i, and sends the smartcard securely to Ui.

2. When receiving SCi^{new}, Ui keys (IDi; PWi) in SCi and biometric information Bi^{new} at the sensor device. Then, SCi calculates $(\psi_i, \theta_i) = GEN(B_i^{new})$, $Ai = h(IDi \| PWi^{new} \| \psi_i)$, $Ei^{new} = \theta_i \oplus h(IDi \| PWi^{new})$, $Ci^{new} = fi^{new} \oplus h(PWi^{new} \| \psi_i)$, $REC^{new} = PWi^{new} \oplus h(IDi \| \psi_i)$, $REGi^{new} = h(IDi \oplus \psi_i)$ and writes (Ci^{new}; Ei^{new}; Ai^{new}; REC^{new}; $REGi^{new}$; GEN(); REP(); h()) into SCi and deletes fi^{new}.

The flaws in this protocol are, 1) It is also suffers from user untraceable attack, because the digestive id MI is calculated in registration phase and used the same MI for each time want to login. 2) If the adversary can compromise a user and read <MI,fi> , the he can able to know the secret of user 'Ki', SIDj and h(ID||T1) using $ki = Li \oplus h(MI \| fi \| T1)$, $SIDj = Pi \oplus h(fi \| t1)$, $h(ID) = Qi \oplus h(ki \| T1)$ while sending login request to GWN. He can also know Kj the secret of SIDj using $Kj = Kij \oplus ki$ while the user receives key establishment details from GWN. Finally he can able to compute session secret key $SK = h(h(ID) \| SIDj \| Ki \| Kj)$ and able to access the communication between user and sensor and vice-versa. 3) It also increases load on GWN when more number of nodes and users are connected, because in each session GWN performs user authentication, node authentication and key establishment between user and node.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

4) It is not suitable forreal-time applications where data must be arrived within thedeadline, because GWN is high speed processing and waitfor node with low speed processing for accept the user'sprivate key and send back the digestive secret sharing keywill be send to user.

IV.DETECT AND DEFEAT TECHNIQUES

The detection and mitigation strategies classified as 1) Use Multi-Data Flow to transmit data in multiple alternative paths to destination. 2) Detection using Acknowledgement from check point nodes or reputation information from neighbor nodes. In the implementation all detection techniques, it have some default assumptions. Some of the assumptions are

- There is a secure communication among nodes in the network.
- The nodes can't be compromised at the time of its deployment.
- The Network fix a threshold value on number of packets dropped normally, used to detect attack occurrence in the network.

A. Detection using Binary search

Presented [9] an algorithm to defend against selective forwarding attacks using binary search in clustered Ad-hoc Network modeled as hierarchical structure. The network uses unicast routing between any two nodes, cluster heads to communicate with other nodes. Sequence number is attached for every packet sent from source to destination. Cluster head maintain a table to store the index of packet transmission for each source and destination pair. It also stores sequence number of packet coming from a given source node. Frequently Cluster head checks the list of sequence numbers stored in its table for each source and destination pair. If it finds malfunctioning of intermediate node, due to number of packets dropped is more than threshold value. Then Control packets and Hello Packets are exchanged along a misbehaving path between the sensor node and the cluster head to detect a compromised node. Cluster head sends Control packet to source node to instruct it , send a fixed number of Hello packets are like ordinary packets, which can be dropped by the malicious node. Now, Cluster head compare the drop rate of Hello packets with threshold value. If there is any anomaly then Cluster head uses binary search algorithm to detect malicious node.

Find_malicious_node (path)
//path* = (i_1, i_2, i_3….. i_h); path *contains malicious node//from source node to cluster head C.
k=path length *//number of nodes from source node to//initiator of the search*
//At the beginning, the initiator is the //cluster head
mid = (l+h)/2 *//calculate mid node between source node//and cluster head to divide the path in half*
if (k is equal to 2) { return l+1;
}
***send controlpkts* from CH to mid node to initiatesearch**
***send* fixed *hello packets* from mid node to CH**
if (number of drop of *hello packets*> threshold) {
path= (i_1,i_2,i_3…..i_{mid})
return (Find_malicious_node (path))
}
else {
path= (i_{mid+1},i_2,i_3…..i_h)
return (Find_malicious_node (path))
}

The advantage of this algorithm is, it can detect multiple malicious nodes, if they exist along the path. Disadvantages are it only detects malicious nodes, which are drop packets from source to Cluster head. It have restricted, there is a unicast routing between any two nodes and Cluster head. It also have communication overhead to transmit more number of Control and Hello Packets when malicious node located just either after source node or before Cluster head and when the path have more number of intermediate nodes.

B. Detect and remove using Modified DSR Algorithm

Presented [11] Modified DSR protocol for detection and removal of selective forwarding attack in Ad-hoc Network. In these IDS nodes are distributed across the network, to cover all the nodes in the network. In DSR (Dynamic Source Routing) protocol the source node has to send Route REQ packet to its entire neighbor node, for find a path to the desired destination. Any one intermediate node which have cached route to the destination or destination node send back reply RREP packet to the source. The misbehaving node participate as legitimate in the route finding process and drops packets passed though it to destination.

To detect selective forwarding attack, the source priorly intimates to the destination the number of packets it wants to send. Let N_S is number of packets send by source, and N_D is number of packets received at destination, then the probability of packets received at destination is computed as $P_D = N_D / N_S$. If P_D is greater than packet loss threshold, the destination starts detection mechanism to determine the malicious node is present in the route. If there is no malicious node, the destination sends a positive acknowledgement to the source. Initially the destination sends a query request packet to the node which is at 2-hop distance towards source node and request for number of packets forwarded to node at 1-hop distance from destination. Based on the reply from 2-hop away node, the destination verifies whether the 1-hop away node forwarded all the packets to destination or not. If not, both 1-hop and 2-hop away nodes moves to suspected list. If Correct, the destination send query packet to 3-hop away node and verify the 2-hop away node is correct or not. The Process continues until reaches source or a node is suspected as malicious.

Now the destination node informs about suspected node to its closest IDS node. The closest IDS node gives intimation to its neighbor IDS nodes. When the source node sends next data packets to the destination, the neighbor IDS of suspected node monitor whether packets are dropped or forwarded. If any of suspected nodes are identified to be dropping data packets, it will be placed in malicious node list. Now the IDS node will send the list of malicious nodes to all its neighbors and malicious nodes are removed from the network.

The merits of this protocol are reduction in packet loss rate due the IDS starts detection when there is anomaly of packet transmission. It enables to detect multiple malicious nodes in the route. The limitations of the protocol are the IDS locations are selected in statistical manner to

ISSN:0971-1260
Vol-22- Issue-14-December-2019

ensure that each node in the network covered by at least one IDS. It is not possible to detect malicious node when the malicious node changes the value sent by source to destination, specifies total number of data packets sent to destination. It is waste of time when there is no more malicious nodes except 1-hop away node due to suspect all the remaining nodes, even though they are correct.

C. Audit-Based Detection Technique

Presented [11] Audit-based Misbehavior detection used to detect and remove a node that reject to forward packets in multi hop ad-hoc networks. It verifies node behavior based on per-packet basis. It detects selective forwarding attacks by allowing the source to perform matching against any desired selective dropping pattern.

System Model: Let P_{SD} is the path from a source S to destination D, known to S of length 'k'. Assume that a set of 'm' misbehaving nodes, $|m| \leq k$, exist along the path. It provides interaction among "Reputation Module", "Route Discovery Module" and "Audit Module" in each node. These three modules interact to detect misbehavior node and discover trust worthy routes and compute the reputation of peers.

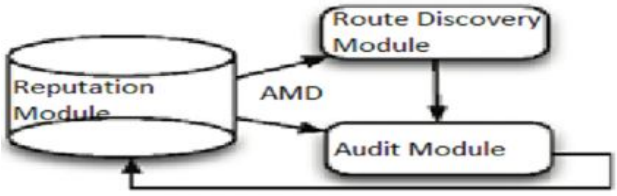

Fig. 10.[11] The AMD system architecture.

The process initiated based on input received from the reputation module. They evaluate reputation of a node by using decentralized approach in ad-hoc networks. A node can evaluate reputation of their peer depends on direct interaction with neighbor nodes and indirect interaction with other nodes.

Evaluation of Node Reputation Value: The node n_i maintains a vector of reputations of all nodes in the network, $Ri(t) = \{r^1{}_i(t), r^2{}_i(t), \ldots, r^N{}_i(t)\}$,$r^j{}_i(t)$ of all nodes $n_j \in N \backslash \{n_i\}$. The reputation values are restricted to the range {0,1}. It uses "Additive Increase and Multiplicative Decrease (AIMD)" algorithm with multiplicative factor $0<\alpha<1$ and additive factor $0<\beta<1$. For each time t, the audit module of node n_i provides a prior evaluation of n_j, the reputation value of $r_i^j(t)$ is computed as

$$r_i^j(t) = \begin{cases} \alpha * r_i^j(t-1) & n_j \text{ is misbehavior node} \\ \min\{ r_i^j(t-1) + \beta , 1.0\} & \text{otherwise} \end{cases}$$

Where $n_i = S$ and $n_j \in P_{SD}$

Due to multiplicative factor the reputation of misbehavior node rapidly declines with repeated packet drops and it requires more time to restore to its reputation due to additive factor. So, it avoids selective forwarding attack by avoid the oscillating between misbehavior and good behavior.

Route Discovery: It is invoked by source node, if it does not have cached path from source to destination using path reputation value. The path reputation is the product of reputation values of all nodes along the path.

Audit Module: It is used to identify malicious node along the path. The source node invokes audit module, if it identify low performance on the path by monitoring the average packet drop rate over a time period't' and drop rate is less than previously defined threshold. The source requests a subset of intermediate nodes along the path to record a digest of set of packets they forward to next hop. Replies from honest nodes leads to detect malicious node using "Renyi-ulam" game. The game comprises of questioner and responder. The responder select a secrete value from a finite set of values. Now the questioner try to that secret value by asking maximum 'q' questions, the responder permitted maximum 'l' lies.

The merits of this scheme are it can detect selective forwarding attacks even though the packets from end-to-end are encrypted, it is applied in multi-channel networks and it enables the concurrent evaluation of behavior of several hops that are not one – hop neighbors. The demerits are it also have communication overhead to transmit reputation vector to other nodes and inclusion of accumulated path reputation field in RREQ and RREP packets while finding path to destination, It evaluate incorrect reputation, when a malicious neighbor could distribute low reputation values of other nodes to remove them from the path.

D. Detection using Fog Computing Based System

Presented [12] a model for identify selective forwarding attacks in Ad-hoc Wireless Sensor Networks. It uses fog computing architecture to implement intrusion detection in the network of mobile nodes. The networks model has two layers. Cloud layer gather information from fog layer, used to obtain dropping patterns of attacks for malicious detection. Fog layer is key layer of this model; it provides, storage, computation and communication services for mobile sensors in the network. The sensor layer comprises of more number of moving sensors.

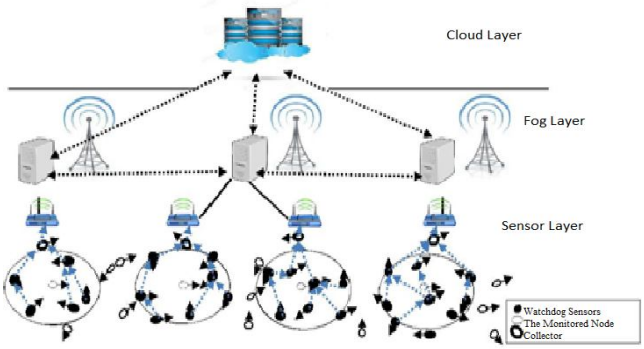

Fig. 11.[12] The Model of Fog Infrastructure.

Each watchdog (monitoring sensor node) observes and store forwarding packets and receiving packets of monitored nodes in its transmission limits. When the monitored node move outside of transmission limit of watchdog, then watchdog transmit information about the node to the collector node. The collector node gives it to the base node, and then gives to Fog server. The Fog server maintains a table that contains the details of packets received and forwarded by monitored nodes. When the monitored node move from transmission area of a Fog server s1, and enters into transmission area of another Fog server s2, the Fog server s2 send a query to Fog server s1 for the information

ISSN:0971-1260
Vol-22- Issue-14-December-2019

about the monitored node. The received information used to compute the dropping probability of the monitored node, to verify whether it is a malicious node or not.

The merits of this method are it provides low latency networking, serving large geographical area. It shows more efficiency with low processing and less battery consumption of watchdog and base station nodes. The demerits are it needs interaction among Fog servers to provide global monitoring which increases communication overhead. It may failure to detect malicious node, when the base station is malicious and not forward information of some sensors to Fog server.

E. Detection using Stochastic Approach

Discussed [13]astochastic Approach for detect selective packet dropping in Mobile Ad hoc Networks. It is a distributed strategy based on Bayesian model to classify node behavior, and Markov chain model to evaluate behavior tracking. They apply fuzzy logic model to identify attacks of periodic packet dropping in ad hoc networks. It consists of three phases as shown in Figure.12. Every node of the network observes its neighbors to gather details about packets transmitted by its 1-hop neighbors, construct a behavior vector of three elements represent the forwarding ratio of three types of packets <DATA, RREQ,RREP>.

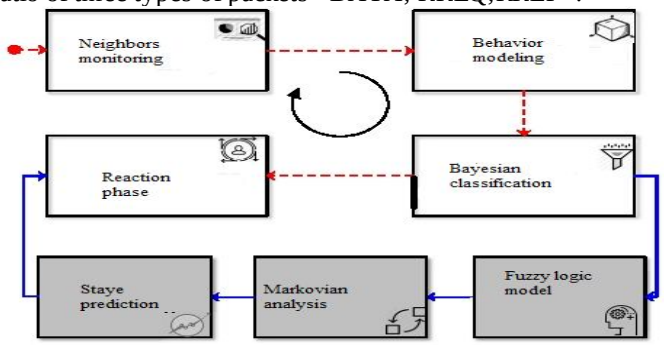

Fig. 12.[13] Phases of Behavior Prediction Approach

Pass the vector as input to Bayesian Classifier to compute the misbehavior level of the node during a time period. The probability value is mapped to misbehavior level of the observed node using Fuzzy Logic model. Depends on sequence of misbehavior levels assigned to observed node during sequence of time slots, a matrix is constructed. Using matrix of probabilities of misbehavior levels of observed node, threshold probability limit of node is calculated using Markov Chain model. Based on threshold the nodes state is predicted and used to estimate the reliability to forward packets. Let FR^1 is forwarding rate of each type of packet during normal conditions i.e without attacks and FR^2 is current forwarding rate of observed node. The misbehavior probability of observed node is estimated by compare $FR^1$and FR^2.Each elementof the behavior vector is set to '1' if corresponding packet type $FR^2 \geq FR^1$, otherwise set to '0'. There are eight behavior vectors due to three types of packets i.e (000) …(111). The classification of node depends on its misbehavior, using Bayesian Theorem (how many times node acts as legitimate and how many times node acts as malicious). The Bayesian classifier uses two thresholds T_{min} and T_{max}. The nodes are classified as legitimate, suspicious, and malicious based on two threshold values.The advantages of this Strategy is improves the accuracy level in the state prediction of each node describes the behavior of node in the network using Fuzzy Logic and Markov Chain Models. But the limitation is each node need to gather information of neighbor nodes and perform computations to calculate probability level of misbehavior of neighbor, leads to delay in data transmission.

V.CONCLUSION

In Ad-hoc Wireless Sensor Networks, it needs to transmit packets in secured and reliable manner. Due to mobility of sensor nodes and deployed in hostile environments, ad-hoc WSNs suffers from active and passive attacks. One of the most effective attacks is Selective Forwarding Attack. In this attack, a malicious node may drop packets selectively which may deterioratesthe integrity of information and not useful at receiver side. It shows more effect on Real-Time networks where information is not useful, if it is not received before dead line. It is complex to detect Selective forwarding Attacks in Ad-hoc WSN due to mobility of nodes and dynamic fluctuations in transmission media. The solution to this attack is either prevents the attackers from access the node in the network based on authentication Protocol or detects the occurrence of attack in the network based information received from nodes in the network and identify malicious node and remove it from network operations. Here, it is discussed and analyzed authentication protocols and detection schemes proposed by earlier researchers to defend and defeat against Selective Forwarding Attacks in ad-hoc Wireless Sensor Networks in table 3 and 4. This will helpful to the readers to have better view on the earlier secure authentication protocols and detection schemes of selective forwarding attacks in WSN and their drawbacks, which will overcome in feature and design efficient authentication protocolsand counter measures against selective forwarding attacks in ad-hoc WSN.

S.No	Proposed Strategy/Protocol	Merits	Demerits
1	Security with Pre-loaded Time Limited Memory Keys (TMLK). [20]	keys are secure and provide mutual authentication, Easy to identify Intruder in the network.	If KDC is blocked from all nodes for time period greater than key life time 'L', then entire network will be destroyed.
2	Biometric Authentication Protocol. [21]	It provides user authentication without transmitting and storing any private information. It is more reliable than conventional password based authentication. It is efficient and light weight in terms of computation and communication.	There is a possibility of session specific information attack, Adversary can compromise user device and extract the information stored in the user device <IDi, Fi> and try to eavesdrop the message RM from Sensor Node to user by compute decryption key Vi=h(IDi‖Fi‖T5) and decrypt message L using Vi as (RM, Ci)=Dvi(L).

ISSN:0971-1260
Vol-22- Issue-14-December-2019

3	Password based User Authentication Protocol. [22]	Provides authentication and key agreement protocol for ad hoc wireless sensor networks. based on dynamic password	An adversary masquerades as a legitimate user and gains access to one or many sensor nodes simultaneously after compromising one of them. After compromising one sensor node, an adversary can masquerade as any legitimate sensor node to which a user is trying to log in.
4	Secure and Efficient Authentication Protocol for Ad hoc WSN. [23]	Provides secure, efficient and flexible authentication protocol using ECC	When the user tries to login with incorrect ID and correct PW, he is authenticated by GWN. So, the protocol does not verify the ID of the user. An adversary can able to guess user's password by extract all the stored information into the user's smart card by conduct online/offline password guessing attack.
5	Untraceable and Anonymous Password Authentication Protocol. [25]	Provides reliable authentication protocol for ad hoc wireless sensor networks to defend against active and passive attacks.	If the adversary can compromise a user and read <MI,fi> , the he can able to know the secret of user 'Ki', SIDj and h(ID‖T1) using ki=Li⊕h(MI‖fi‖T1),SIDj=Pi⊕h(fi‖t1),h(ID)=Qi ⊕h(ki‖T1) while sending login request to GWN. He can also know Kj the secret of SIDj using Kj=Kij⊕ki. Finally he can able to compute session secret key SK=h(h(ID)‖SIDj‖Ki‖Kj) and able to access the communication between user and sensor and vice-versa.

Table.3. Analysis of Authentication Protocols

S.No	Proposed Technique/Scheme	Merits	Demerits
1	Detection using Binary search. [9]	It can detect multiple malicious nodes, if they exist along the path.	It only detects malicious nodes, which are drop packets from source to Cluster head.
2	Detect and remove using Modified DSR Algorithm. [10]	The merits of this protocol are reduction in packet loss rate due the IDS starts detection when there is anomaly of packet transmission. It enables to detect multiple malicious nodes in the route.	The IDS locations are selected in statistical manner to ensure that each node in the network covered by at least one IDS. It is not possible to detect malicious node when the malicious node changes the value sent by source to destination, specifies total number of data packets sent to destination.
3	Audit-Based Detection Technique. [11]	It can detect selective forwarding attacks even though the packets from end-to-end are encrypted, it is applied in multi-channel networks and it enables the concurrent evaluation of behavior of several hops that are not one – hop neighbors.	It also have communication overhead to transmit reputation vector to other nodes and inclusion of accumulated path reputation field in RREQ and RREP packets while finding path to destination, It evaluate incorrect reputation, when a malicious neighbor could distribute low reputation values of other nodes to remove them from the path.
4	Detection using Fog Computing Based System. [12]	It provides low latency networking, serving large geographical area. It shows more efficiency with low processing and less battery consumption of watchdog and base station nodes.	It needs interaction among Fog servers to provide global monitoring which increases communication overhead. It may failure to detect malicious node, when the base station is malicious and not forward information of some sensors to Fog server.
5	Detection using Stochastic Approach. [13]	It improves the accuracy level in the state prediction of each node describes the behavior of node in the network using Fuzzy Logic and Markov Chain Models.	In this each node need to gather information of neighbor nodes and perform computations to calculate probability level of misbehavior of neighbor, leads to delay in data transmission

Table.4. Analysis of detection Techniques

REFERENCES

[1] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, 1(2-3):293–315, 2003.

[2] Leela Krishna Bysani and Ashok Kumar Turuk 'A Survey On Selective Forwarding Attack in Wireless Sensor Networks" in International Conference on Devices and Communications ,24-25 February 2011 Mersa, India.

[3] Wazir Zada Khana, Yang Xiangb, Mohammed YAalsalem,Quratulain Arshad," The Selective Forwarding Attack in Sensor Networks: Detections andCountermeasures" International Journal of Wireless and Microwave Technologies (IJWMT), Vol.2, No.2**,** April 2012, pp.33-44.

[4] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. An efficient countermeasure to the selective forwarding attack in wireless sensor networks. pages 1 –4, oct. 2007.

[5]Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2006.IPDPS 2006. 20th International*, page 8 pp., 2006.

[6]Ji Won Kim, Soo Young Moon, Tae Ho Cho, Jin Myoung Kim, Won Tae Kim, Seung Min Park, "Control Method of Checkpoint Node Selection Using a Fuzzy Rule System and Feedback in CHEMAS" Advanced Communication Technology (ICACT), 13th International Conference ,Feb 2011,pp.584-87.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

[7]Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin," Lightweight defense scheme against selective forwarding attacks in Wirelesssensor networks." 978-1-4244-5219-4/09 pages 226 – 232, oct. 2009.

[8] Jeremy Brown and Xiaojiang Du. Detection of selective forwarding attacks in heterogeneous sensor networks. In *ICC*, pages 1583–1587, 2008.

[9] Sawati Mukherjee, Matangini Chattopadhyay, samiran Chattopadhyay " Detection of Selective Forwarding Attack in Ad hoc Networks using Binarysearch" in International Conference on Emerging Applications of Information Technology. 978-1-4673-1827-3, 2012.

[10] M.Mohanapriya, Ilango Krishnamurthi "Modified DSR protocol for detection and removal of selective black hole attack in MANET " in Journal onComputers and Electical Engineering, Vol 40, no.2, pp. 530-538, Feb 2014.

[11] Y.Zahang,L.Lazos,W.Kozma "AMD: Audit based Misbehavior Detection in Wireless Ad Hoc Networks " in IEEE Transactions on Mobile Computing,Vol 15, no.8, pp. 1893-1907, 1 Aug 2016.

[12] Qussai Yaseen, Firas AlBalas and Yaser Jaraweh "A Fog Computing Based Systems for Selective Forwarding Detection in Mobile Wireless Sensor Networks" in IEEE 1st International Workshops on Foundations and Applications of Self Systems, 978-1-5090-3651-6/16,2016, pp 256-262.

[13] Mohammad Rmayti, Rida Khatoun, Youcef Begriche, Lyes Khoukhi,Dominique Gaiti " A Stochastic Approach for Packet Dropping Attacks Detection in Mobile Ad hoc Networks" *Computer Networks*,vol 121, July 2017,pp 53-64.

[14] Chunxiao Chigan, Yinghua Ye, Leiyuan Li " Balancing security against Performance in Wireless Ad Hoc and Sensor |Networks " *0-7803-8521-7/04, 2004.*pp 4735-4739.

[15] Ismail Mansour, Damian Rusinek, Gerand Chalhoub " Multihop Node Authentication Mechanisms for Wireless Sensor |Networks " *ADHOC-NOW 2014, LNCS 8487,* 2014,pp 402-418.

[16] Harald Vogt " *Increasing Attack Resiliency ofWireless Ad Hoc and Sensor Networks*" *International Conference on Distributed Computing Systems,1545-0678/05, 2005*.

[17] N. Boudriga,M. Baghdadi,M. S. Obaidat" A New Scheme for Mobility, Sensing, and Security Management in Wireless Ad Hoc Sensor Networks" Proceedings of the 39th Annual Simulation Symposium (ANSS'06),0-7695-2559-8/06,2006.

[18] Sk.Md.Mizanur Rahman, Nidal Nasser " Private Communication and Authentication Protocol for Wireless Sensor Networks" 978-2-9532443-0-4,2008.

[19] A.Ali, N.Fisal " Security Enhancement for Real-Time Routing Protocol in Wireless Sensor Networks" 978-1-4244-1980-7,2008.

[20] Vadim Kimlaychuk" Security in ad-hoc sensor networks with pre-loadedtime limited memory keys" , 978-1-4244-9352-4/11, 2011 IEEE.

[21] Ohood Althobaiti, Mznah Al-Rodhaan,and Abdullah Al-Dhelaan "An Efficient Biometric Authentication Protocol for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Volume 2013, Article ID 407971, 13 pages.

[22] M. Turkanovic and M. Holbl, "An improved dynamic password-baseduser authentication scheme for hierarchical wireless sensor networks,"Electron. Elect. Eng., vol. 19, no. 6, pp. 109–116, 2013.

[23] Chin-Chen Chang, Hai.-Duong. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks" , IEEE Transactions on Wireless Communications 15(1)(2016)357–366.

[24] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credentialbased security scheme with mutual authentication and key agreement for wireless sensor networks", Sensors, vol. 13, pp. 9589–9603, Jul. 2013.

[25] Ruhul Amin, SK Hafizul Islam, Neeraj Kumar, Kim-Kwang Raymond Choo,"An Untraceable and Anonymous Password Authentication Protocol for Heterogeneous Wireless Sensor Networks", Journal of Network and Computer ApplicationsVolume 104, 15 February 2018, Pages 133-144.

[26] R. Amin, G. P. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Networks 36 (2016) 58–80.

[27] Y. Dodis, L. Reyzin, A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", International conference on the theory and applications of cryptographic techniques, Springer, 2004, pp. 523–540.

ABOUT THE AUTHORS

Mr. A.V.S.Sudhakara rao obtained his B.Tech (CSE) from GIET, Rajahmundry affiliated to JNTUH, Hyderabad and M.Tech (CSE) from University College of Engineering, JNTUK, Kakinada. Currently pursuing Ph.D (CSE) from Jawaharlal Nehru Technological University Ananthapur, Ananthapuramu, A.P. , India. Currently he is working as Associate Professor in CSE Department of St. Ann's College of Engineering and Technology, Chirala. He is also qualified in UGC-NET. His Spcialization includes MANETs and Algorithm Analysis. He is a life member of CSI.

Dr. M.Sreenivasulu is presently working as Professor and HOD of Computer Science and Engineering Department in KSRM College of Engineering, Kadapa,A.P., India. He did his B.Tech in CSE from Koneru Lakshmaiah College of Engineering, VaddeswaramGuntur affiliated to Nagarjuna University. M.tech in CSE from Jodavpur University, Calcutta, West Bengal. Ph.D. in CSE from Jawaharlal Nehru Technological University Ananthapur, Ananthapuramu, A.P. , India. He has 25 years of Teaching experience and 15 years of Research experience. His areas of interest includes Computer Networks, Wireless Networks and Cloud Computing. He is member of IEEE, ISTE and IEI.