International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 3, May-June 2016 **ISSN 2278-6856**

Attack Resilient Dynamic Key Management Scheme for Wireless Sensor Networks

Prof. Bachala Sathyanarayana [1], C.Krishna Priya[2]

[1]Professor, Department of Computer Science and Technology,
Sri Krishnadevaraya University, Anantapuram, Andhra Pradesh , India

[2] Research Scholar, Department of Computer Science and Technology,
Sri Krishnadevaraya University.

Abstract

Most of the existing schemes for key management are static and meant for static WSN. However, dynamic key management for dynamic WSN is the potential research area to safeguard WSN from adversaries besides being flexible. The existing schemes in WSN focused more on the energy efficiency rather than security. To address this problem, earlier we implemented a dynamic key management scheme for dynamic WSN with energy efficiency. It is cluster based and broadcast authenticated which could handle dead nodes and compromised cluster head efficiently. In this paper we proposed our security scheme to make it resilient to various attacks like black hole, carousel, rushing, wormhole, Sybil and flooding attack. Extensive simulations performed using NS-2 Network Simulator showed that the proposed approach is capable of preventing such attacks in WSN. The proposed scheme shows significant performance improvement in terms of throughput, energy efficiency, delay performance, dropping and packet delivery ratio.

Keywords: Wireless Sensor Network (WSN), security, dynamic key management, energy efficiency, attack resiliency

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are popular in civilian and military applications. Civilian applications are monitoring patients in healthcare domain, surveillance and studying wildlife habitat to mention few. Military applications are like monitoring border areas, surveillance for finding enemy movements and so on. WSNs are also well known for vulnerability causing potential security threats. Since WSN is used for pervasive computing, the low power or resource constrained nature of network and the mobility are two important reasons for security threats. Securing communications in WSN in energy efficient fashion is essential. In [1] we made a review of efficient key management schemes for secure routing. Earlier we proposed
an energy efficient and dynamic key management (EEDKM) scheme for WSN [2] and explored how the scheme could provide security besides being energy efficient. The scheme
was cluster-based and it has three layers. The first layer is base station (BS) the second layer is cluster head (CH) while the third layer is sensor node (SN) which actually collects data and forwards it to BS through a pre-defined mechanism. The scheme consumes less energy as it rotates cluster heads randomly. The scheme is dynamic and it works for dynamic WSN. The underlying key distribution scheme is computationally efficient besides reducing energy consumption. Both energy efficiency and security were achieved.
In this paper our focus is on exploring different types of attacks that can be modeled and prevented. The attacks we considered include black hole attack, flood attack, carousel attack, wormhole attack, Sybil attack and rushing attack.
The work done by us in [2] was extended further in order to study the effectiveness of our scheme and its robustness towards these attacks. The following sub sections provide details of the attacks.

1.1 Potential Threats to WSN Security

WSN is vulnerable to many attacks such as black hole attack, worm hole attack, flooding attack, Sybil attack, Carousel attack, and rushing attack.

1.1.1 Black Hole Attack

A black hole attack is characterized by a node dropping all packets that come in its way. Such node acts like a black hole. The attack will have much more impact on the network when the black hole node is the connecting node of two connecting components of the network. This attack is illustrated in Figure 1 (a).

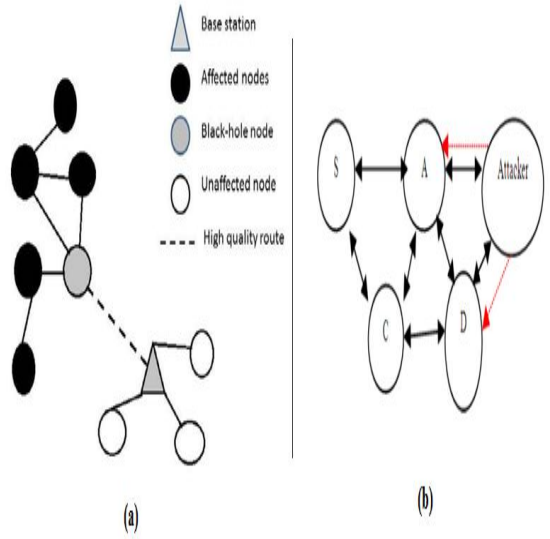

Figure 1-Shows black hole attack (a) [3] and flooding attack (b) [4]

1.1.2 Flooding Attack

As shown in Figure 1 (b), it is an attack in which a node floods network with message claiming that the path through it is a high quality route. Believing it, every node tries to send their packets through this node. In the process, some nodes might send packets with destination are not in the reach of attacker node as the attacker node convinces that all nodes are its neighbors. Moreover the traffic generated by the attacker node is not genuine.

1.1.3 Rushing Attack

Generally, before sending data to destination a node establishes route with the destination. A RREQ message is broadcasted by sender node to its neighborhood. Valid routes come back to the source with RREP with correct route information. However, some protocols follow mechanism known as duplicate suppression which is exploited by adversaries to launch rushing attack. Rushing attack is an attack in which an attacker forwards with RREP with malicious intentions on behalf of a legitimate node without following proper procedure. The attacker node filters packets before sending to correct node. Therefore it appears from outside that everything is done as per protocol. However, the attacker node really caused delay in data transmission. This attack is illustrated in Figure 2 (a).

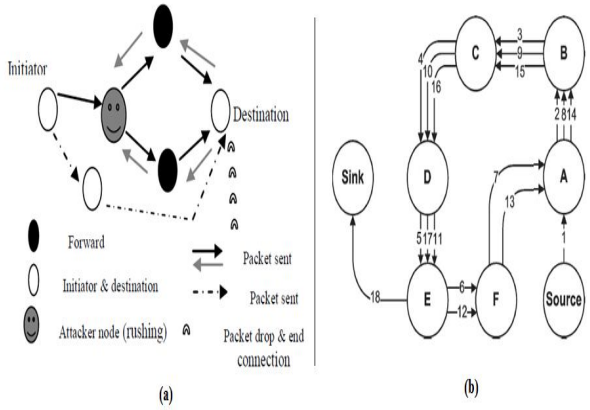

Figure 2 Rushing attack (a) [5] and carousel attack (b) [6]

1.1.4 Carousel Attack

As shown in Figure 2 (b), it is an attack which causes unnecessary traffic in network causing energy depletion. Malicious node makes a loop in routing where packets are flows through the routes iteratively before they are sent to destination finally. This attack causes lot of network traffic thereby causing reduction of energy levels in the network. This leads to reduction of lifetime of network.

1.1.5 Wormhole Attack

It is an attack in which an adversary captures data packets at one node of the network (origin of the packets) and tunnels the packets to a destination point. From the destination point, the adversary retransmits the data to neighborhood nodes as shown in Figure 3.

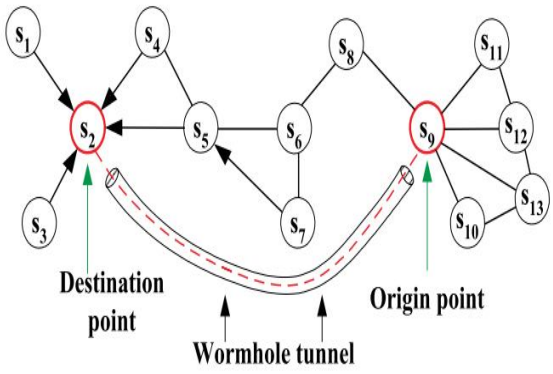

Figure 3 – Shows wormhole attack [20]

This kind of attack can be launched without actually compromising a node in the network. Its success is based on the strength of the cryptographic primitives being used in the network. Hence it is difficult to detect such attacks

1.1.6 Sybil Attack

It is an attack in which a malicious node is able to forge many identities illegally as shown in figure 4. Thus the malicious node is capable of creating misjudgments among the legitimate nodes in the network. Especially in WSN Sybil attacks are very harmful. Stated differently the Sybil attack is the process of forging identities of nodes in WSN. Here a Sybil node is nothing but the additional identity of misbehaving node [19].

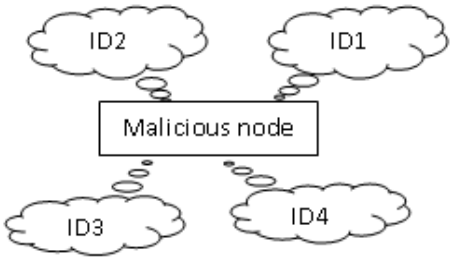

Figure 4- Malicious node announcing its multiple identities

Our contributions in this paper are described here. We enhanced our key management scheme [2] to validate its robustness against the aforementioned attacks. We proposed and implemented various approaches to counter the attacks and ensure that the WSN with our scheme remains secure. Our extensive simulations using NS2 reveal that the proposed defence mechanisms that work with our key management scheme are robust to the attacks mentioned above. The remainder of the paper is structured as follows. Section II reviews relevant literature on key management schemes and attacks in WSN. Section III presents the proposed mechanism to defend various kinds of attacks. Section IV presents simulation results. Section V concludes the paper besides providing directions for future work.

2. RELATED WORKS

This section reviews literature on various attacks and counter measures. Especially it throws light into six attacks in WSN such as black hole attack, flooding attack, rushing attack, carousel attack, worm hole and Sybil attacks.

2.1 Black Hole Attack

Ramaswamy *et al.* [7] proposed a mechanism that addresses cooperative black hole attack. It is an attack that has high impact on the network as this is launched by multiple black holes with coordination among them. Their solution finds a safe route and avoids cooperative black hole attack. Anitha and Vasudevan [8] proposed a certificate based authentication mechanism for preventing black hole attack in multicast routing protocols. The nodes in the network coordinate each other and by issuing certificates. There is no need for centralized authority to issue certificates. The solution is associated with a protocol named On Demand Multicast Routing Protocol (ODMRP). Their solution could reduce 20% packet drop due to black hole attacks. Besides, the solution was made flexible so as to prevent other routing attacks as well. Ruiz *et al*. [9] proposed an approach that can inject black hole attack into network. The attack was injected between two nodes whole path is publicized as best path to other nodes. Roopak and Reddy [10] studied performance of AODV protocol under black hole attack. Then they evaluated the work using measures like end to end delay, throughput and PDF. Under the black hole attack, all these metrics showed that PDF and throughput were decreased while the end to end delay has decreased.

2.2 Flooding Attack

Madhavi and Duraiswamy [11] proposed a methodology for handling flooding attack in WSN. The performance parameters considered include throughput, delay and packet delivery ratio. Their experiments with a new algorithm associated with AODV could prevent flooding attacks besides reducing control overhead by 2%. Choubey et al. [12] focused on hello flooding attack and provided defence mechanism through probabilistic secret sharing protocol besides employing multipath routing to multiple base stations and bidirectional verification to defend such attacks. Sawant and Rawat [13] studied Denial of Service (DoS) flooding attacks in mobile networks. They described how the attacks are made and also provided counter measures. They suggested using secure routing protocols to void such attacks.

2.3 Rushing Attack

Rushing attacks were explored in [14]. Especially the impact of rushing attacks in multicasting of on mobile networks was studied. The success rate of attack, as revealed in the research paper, is influenced by the node positions. Another fact in the research is that the attack made near receiver is likely obtaining more success rate when compared with other two positions such as near sender and anywhere. Suthar and Panchal [15] proposed a prevention mechanism for rushing attack by using a modified AODV protocol. Since rushing attack is based on duplicate suppression mechanism, it is possible to avoid it of mitigate it by altering an appropriate property of AODV protocol.

2.4 Carousel Attack

Vasserman and Hopper [16] for the first time explored more on Carousel attack which drains energy from WSN. The Carousel attack is the attack in which malicious

packets make their way around a loop before reaching base station. This causes unnecessary traffic and results in energy wastage. They provided a counter measure to Carousel attack by letting forwarding nodes to check source routes for loops. Though this approach increases overhead, it can prevent such attacks effectively. Kim [17] used the term carousel in different meaning. He intended to describe a data structure that contains shared secret and explored carousel guessing attack and its prevention mechanism. Manimala and Devapriya [18] proposed a method known as EWMA for tolerating Carousel attacks. This approach ensures that the packets sent from source to destination do not involve in unnecessary looping prior to reaching base destination. In this paper we proposed a methodology for energy efficient solutions to counter all these attacks.

2.5 Wormhole and Sybil Attacks

Lazos et al. [20] explored the prevention mechanism of Wormhole attack which is caused due to tunneling of data from origin to destination node and then retransmit to the neighbors of destination node. They followed a graph theoretic approach to prevent the attack. Zhang et al. [19] proposed a method for identifying and preventing Sybil attack in WSN. Their approach was to identify a node which will make use of multiple identities and prevent the attack from being successful.

3. PROPOSED SYSTEM

The proposed scheme is known as Attack Resilient Dynamic Key Management (ARDKM). It is based on a WSN with three layers. The layers include base station (BS), cluster head (CH) and sensor node (SN). Sensor nodes can perform sensing activities and send data to BS in a systematic fashion. There is communication between SN and CH. Two SNs can also communicate with each other. The communication between two sensors, between sensor node and cluster head and between the cluster heads and base station are secured using our key management scheme proposed in [2] where more details can be found. The technical details of network initialization, key establishment in terms of cluster key establishment, and master key establishment, periodic key updating, node addition and deletion mechanisms, and CH replacement can be found in our scheme [2]. In this paper we extend the scheme and our focus is on various attacks such as black hole attack, rushing attack, flooding attack and carousel attack. To handle these attacks efficiently and ensure that the scheme remains energy efficient and attack resilient, we implemented different mechanisms or algorithms as explained below. Before detailing into attack prevention, we show the architectural overview of our framework

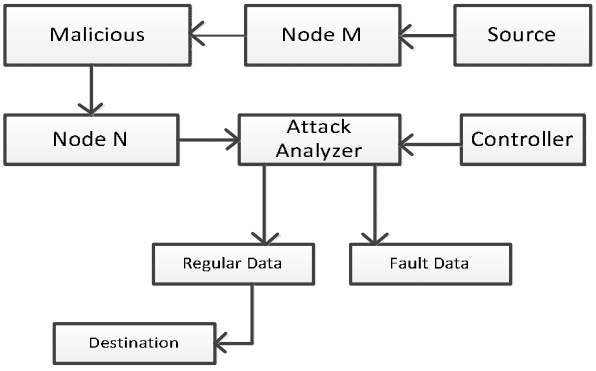

Figure 5 – Overview of the architecture

As shown in Figure 5, the data is transmitted from source to destination through mediate nodes, where the nodes may include malicious nodes also. While transmitting the data in the network, attack analyzer must analyze the time and amount of data transmitting from source to destination. If the node transmits the data to wrong node instead of destination node, miss-judgment, path failure, data reached after timeout including fault data with regular nodes, packet dropping then message goes to controller which controls the flow, attack analyzer checks the path set into proper communication. All the attacks that are prevented in this paper are given below.

3.1 Attack Detection Mechanisms

This subsection provides detection mechanisms for black hole, flooding and rushing attacks.

3.1.1 Detection of Black hole Attack

Data is sent from source to destination through intermediate nodes. Number of sent out RREQ and received RREP messages are represented appropriately. The average of difference in each time slot is represented as DstSeq. The average of the difference between the DstSeq in RREQ message and the one held in the list are calculated. When sending or forwarding a RREQ message, each node records the destination IP address and the DstSeq in its list.

When the WSN is considered to have a state for each node a multi-dimensional feature vector is used to represent it. The destination sequence number is considered in order to detect black hole attack. In a normal state, the sequence number changes as per the traffic conditions. However in an abnormal state, the sequence number increases abnormally. Based on this, the following expressions are used to model and detect the attack.

In the i^{th} time slot, the traffic flow at each node in WSN is considered to be a three-dimensional vector xi = (xi_1, xi_2, xi_3). The nodes with normal state generally have similar feature space while the nodes with abnormal state deviate much. The mean vector is computed as follows.

$$\bar{x}^D = \frac{1}{N}\sum_{i=1}^{N} x_i$$

Then, the distance from a sample x to the mean vector $\bar{x}^D$ is computed as follows.

$$d(x) = \|x - \bar{x}^D\|2$$

Based on the threshold, the occurrence of the attack is determined.

$$\begin{cases} d(x) > T_h & : \ attack \\ d(x) \le T_h & : normal \end{cases}$$

The projection distance with maximum value is extracted as threshold value.

$$T_h = d(x_I) \text{ , Where I= max of } d(x_i)$$

3.1.2 Detection of Rushing Attack

Bayes' theorem is used to detect rushing attack. Here S represents that there is no attack associated with a node. In the same fashion Pos and Neg indicate positive and negative values for the attack. The Bayes' theorem is as follows.

$$P(S|Pos) = (P(S)P(Pos|S))/(P(S)P(Pos|S) + P((\bar{S})P(Pos|\bar{S})))$$

P(S/ Pos) → Probability of occurrence of node test is only positive selfishness (Which is attack occurrence). To find the occurrence of selfishness (attack) in the network is nothing but mutual occurrence of selfishness from overall selfishness in the WSN.

$$S = (P(S)P(Pos|S))/(P(S)P(Pos|\bar{S}))$$

To find the probability of attack:

$$P(S|Pos) = S/(1+S)$$

Let R and $\bar{R}$ be the events representing regular and not regular nodes respectively. Not regular means attack. The normal density P(x | R) can be computed using prior probabilities such as P(R) and P ($\bar{R}$). Node density is nothing but simulation evaluated how well connected a system of randomly placed nodes are for different node densities and network sizes.

$$P(X/R) = \frac{1}{\sigma_R\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu_R}{\sigma_R})2} \text{ and}$$

$$P(X/\bar{R}) = \frac{1}{\sigma_{\bar{R}}\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu_{\bar{R}}}{\sigma_{\bar{R}}})2}$$

σ_R, μ_R is used for the summation notation & detection of attack at regular node respectively.

When continuous version of Bayes' theorem is adapted:

$$P(R/X) = \frac{P(R)P(\frac{X}{\bar{R}})}{P(R)P\left(\frac{X}{\bar{R}}\right) + P(\bar{R})P(\frac{X}{\bar{\bar{R}}})}$$

3.1.3 Detection of Flooding Attack

A simple mathematical analysis of flooding attack is as given below. The success ratio represented by S is used to compute the ratio of Route Request Flooding Defense (RRFD) against Route Request Flooding Attack (RRFA).

A node has to authenticate routing messages from any node in the network except malicious node. This node never forwards the required data to destination

$$S = 1 - \frac{\text{Number of forged RREQs forwarded by node if RRFD is used}}{\text{Total number of forged RREQs forwarded by node if RRFD is not used}}$$

Since the value of S changes from time to time based on the attack, S_n is defined as success rate at $(n+1)^{th}$ attempt of an attacker. Let R_i is the success rate of WSN node in defending RRFA between i^{th} and $i+1^{th}$ route discovery cycle. Let x be the number of transmitted RREQs.

$$R_i = 1 - \frac{x}{(1+\min(2^{i-1},64))x} = 1 - \frac{x}{(1+\min(2^{i-1},64))}$$

$$S = 1 - \frac{nx}{ny + \varepsilon_{i=1}^{n} \min(2^{i-1},64) * y}$$

R_i is $\frac{1}{2}$ since one RDC of RREQs is dropped during the interval between the start of the first and just before the start of the second successful RDC. Where i=1 and x=1.

3.2 Algorithms Implemented

This sub section provides the algorithms that are employed to handle the aforementioned attacks on WSN

Algorithm to prevent Black Hole attack

```
1  Source node broadcasts RREQ
2  Source node receives RREP
3  IF RREP is from the destination or reliable node Then
4      Route Packets to DN
5      ELSE
7      For each intermediate node in all nodes
8          Send id of intermediate node and further request to next hop node
9          Receive FRp and next hop node of current next hop node
10         Receive data routing info of intermediate node, next hop of next hop node
11         IF next hop node is reliable Then
12             Use data routing info for checking intermediate node for black hole
13             IF intermediate node is not black hole Then
14                 Route data packets
15             ELSE
16                 Consider it Insecure Route
17                 Consider intermediate node as black hole
18                 Consider nodes from intermediate node to RREP generator in reverse path as
19                 black holes
20             END IF
21         ELSE
22             Current intermediate node = next hop node
23         END IF
24 END IF
```

Figure 6 – Algorithm to prevent black hole attack

As shown in Figure 6, the black hole attack is prevented by collecting multiple RREP messages for multiple redundant paths to destination besides buffering packets in order to use them when safe route is found in order to withstand black hole attack. Here is the full description of it. After getting route request from the source node, it is verified whether the data reaches to the destination through reliable nodes. Towards this end, multipath is established and buffer of data is maintained. Then the route request is rebroadcasted to destination. Further reply, next hop node of the current node and data routing information are considered. Hop of data transferring from source to destination is true or false is verified. If it is true, the black hole attack is identified. If not the process is repeated. When an attack is suspected, that path is blocked and data packets are sent in different path.

Algorithm to prevent flooding attack

```
1  Node floods RREQ
2  RREQ count is made at each node
3  IF count > threshold THEN
4      Suspect flooding attack
5      Identify error free route
6      Forward data packets
7  ELSE
8      Forward data packets
9  END IF
```

Figure 7 – Algorithm to prevent flooding attack

With respect to flooding attack, it is evident that route request is flooded into network by a malicious node. At each node route request is counted. Then the count is verified against a threshold value. Based on the threshold value, the flooding attack is identified and it is handled by finding an error free route for forwarding packets.

Algorithm to prevent Rushing attack

```
1   Source node broadcasts RREQ
2   Source node receives RREP
3   IF node is reliable Then
4       Route data packets
5   ELSE
6       For each Unknown source node
7           Use middle node to send packets to next node
8           Receive reply and routing info of all nodes
9           Validate the route and each node
10          IF data is valid and route is known THEN
11              Route data packets
12          ELSE
13              Suspect rushing attack launched by middle node
14              Fame information is detected
15          END IF
16          IF node need prevention Then
17              Check neighbour node to find node delay
18              Update route with intermediate node
19              Send route information to controller
20              Sender gets route information
21              Discover secure node
22          END IF
23      END IF
24  END FOR
```

Figure 8 – Algorithm to prevent rushing attack

As shown in Figure 8, a node receives RREQ and unicasts it to its neighbour. Then the RREQ packet is verified with time interval. Is there is discrepancy in time interval, it updates routing table and turns of promiscuous operations of the node. The check request packet is broadcasted. If the packet is received from reliable node, it is ok otherwise an alternative path is selected. In essence this mechanism identifies a node that rushes communication without following protocol formalities.

Algorithm to prevent Carousel attack

```
1  Source node broadcasts RREQ
2  Source node receives RREP
3  IF RREP is from destination or a reliable node THEN
4      Route data packets
5      Source node broadcasts RREQ
6      IF packet is from destination or a reliable node THEN
7          Route data packets
8      Else
9          Send further request and identity of the packet already received for further request, Data Routing
   Information entry for next hope node's next hop.
10 Put a data routing information entry for current intermediate node
11 IF next hop node is a reliable node THEN
12     Check intermediate node for carousel using data routing information entry
13     IF intermediate node is not caurosel THEN
14         Route data packets
15     ELSE
16         Consider route as insecure
17         Consider intermediate node is a caurosel
18         All the nodes along the reverse path from intermediate node to the node that generated
             RREP is caurosel
19     END IF
20 ELSE
21 Current intermediate node = next hop node
22 END IF
23 Repeat steps for all intermediate nodes
```

Figure 9 – Algorithm to prevent carousel attack

With respect to carousel attack it is evident that the there is a mechanism to know whether a packet is repeatedly forwarded to intermediate nodes before sending to actual destination. This is done by maintaining a count of the visit of a packet to a node. This information updated in the routing table can help identify the carousel attack. This attack is basically to cause unnecessary traffic by sending packets to a set of nodes before sending it to destination. The proposed mechanism takes care of this kind of attack and ensures that the energy of the network is optimally utilized. Figure 9 shows an algorithm to prevent carousal attack.

```
1. start
2. Generate a data request (REQ) to neighbor node
3. setting the time to reach REQ to destination
4. REP to REQ from respective node
5. If
5.      {
6.              REP arrived before timeout t1<T
7.              set the link status as proven
8.      }
9. else t1>T
10.     {
11.             set the link path as suspicious
12.             stop the communication with the link.
13.     }
14.stop
```

Figure 10 – Shows prevention for wormhole attack

As can be seen in Figure 10, it is evident that the attack is detected based on the time flag set in the communication process. If the REQ reaches destination in the given time, it needs to be considered as legitimate else it has to be suspected and communication to such node has to be stopped.

```
1.Start
2.Perform R random walks with length l
3.Receive Reply message
        REP message with MAC Address
        each node with MAC Address for different routes
4. compare MAC respective IP Add
5.if
6.      {
7.      Mac add matches with different IP
8.      node is Sybil
9.      }
10.else
11.     REP accepted
12. Stop.
```

Figure 11 – Shows prevention for Sybil attack

As shown in Figure 11, the Sybil attack is based on the identification of MAC address. When there is evidence that the node is using forged identity then it is considered to be the node involved in Sybil attack. If not the node is considered to be a legitimate node and the communication is allowed.

4. SIMULATION AND RESULTS

Simulation study has been made in order to realize the proposed approach for efficient key management. The simulation environment is as given below.

Table 1: Simulation environment details

PARAMETER	*SPECIFICATION*
Simulation tools used	*NS2 Network Simulator (ns-2.35)*
Simulation time	*10 sec, 20 sec, 30 sec*
Number of nodes	*100,200,300,..., 800*
Transmission range	*250m*
Maximum speed	*0-20 m/sec*
Application traffic	*CBR [constant bit rate] [20]*
Packet size	*512bytes*
Node mobility model	*8 packets/sec*
Protocol	*AODV*

The simulation results pertaining to performance level of the proposed method and the other attributes like packet delivery ratio, packet delay and packet dropping were recorded. The results are as shown below.

Table 2: Simulation result

Energy Consumption							
N/W size	100	200	300	400	500	600	700
EEDKM	10	13	19	28	36	48	62
Proposed	3	7	11	21	28	40	51
BA	15	19	25	32	40	55	65
Network Output							
N/W size	100	200	300	400	500	600	700
EEDKM	120	170	250	400	550	700	800
Proposed	200	250	380	540	700	820	930
BA	80	120	160	250	320	430	650

Performance on Dropping							
Time	5	10	15	20	25	30	35
EEDKM	580	490	380	320	270	210	160
Proposed	500	400	300	250	200	150	100
□BA	660	550	430	390	330	270	200
Performance Analysis on Delay							
Time	5	10	15	20	25	30	35
EEDKM	800	710	600	390	310	180	160
Proposed	700	650	520	320	220	120	110
BA	900	800	720	540	425	280	230

Performance Level Of PDR							
Time	5	10	15	20	25	30	35
EEDKM	40	45	60	70	75	87	90
Proposed	50	55	72	78	85	95	100
BA	30	35	48	54	63	68	75

As can be seen in Table 2, it is evident that the simulation results pertaining to delay performance, packet delivery ratio, packet dropping, throughput and energy consumption.

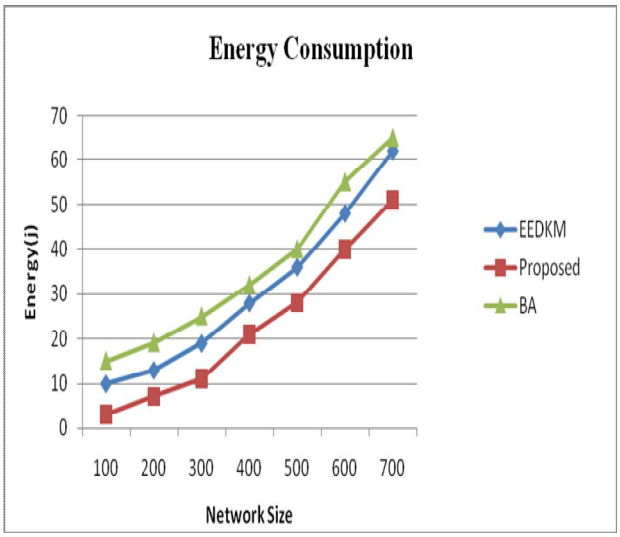

Figure 11 – Comparison of energy consumption

As shown in the above figure, the horizontal axis represents network size while the vertical axis represents energy consumption. The results revealed that there is energy consumption trend in the increasing order of network size. However, the proposed scheme shows better performance with decrease in energy consumption when compared with other schemes.

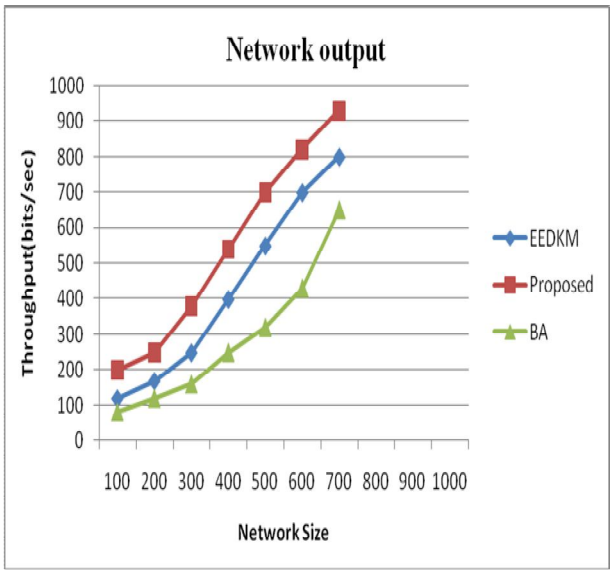

Figure 12 – Comparison of throughput performance

As shown in the above figure, the horizontal axis represents network size while the vertical axis represents throughput. The results revealed that the throughput of proposed increases in the increasing order of network size when compared with EEDKM and BA.

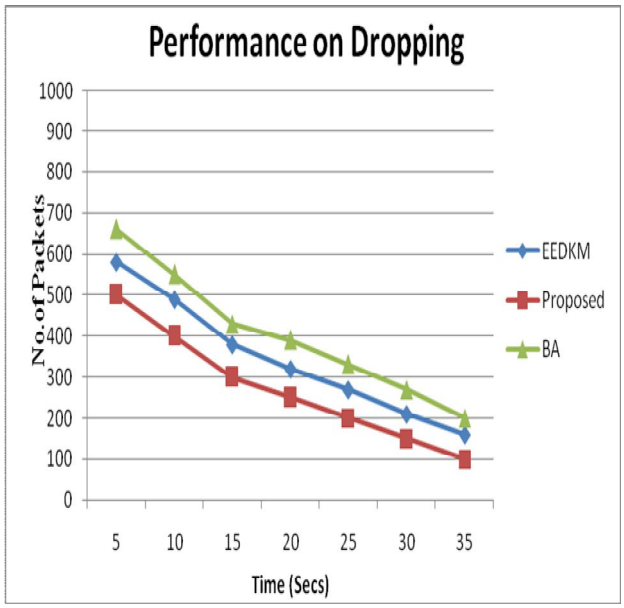

Figure 13 – Comparison of packet dropping

As shown in the above figure, the horizontal axis represents simulation time while the vertical axis represents number of packets dropped.. The results revealed that there is decreasing trend of packet dropping as simulation time goes on. However, the proposed scheme shows decrease in packet dropping which is better performance when compare to existing schemes.

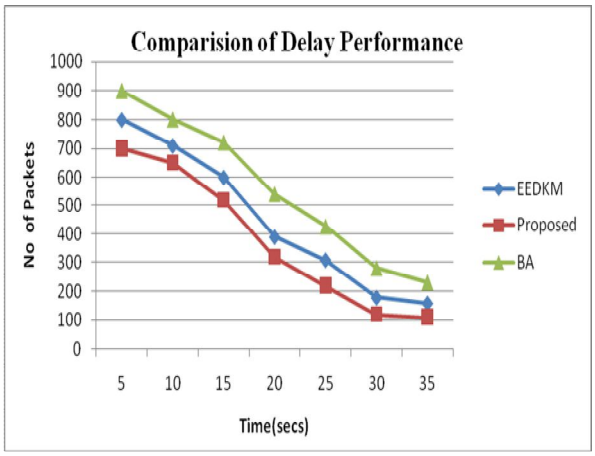

Figure 14 – Comparison on delay performance

As shown in the above figure, the horizontal axis represents simulation time while the vertical axis represents number of packets. The results revealed that the delay is decreased as simulation time goes on. That is the proposed scheme shows better performance when compare to other schemes.

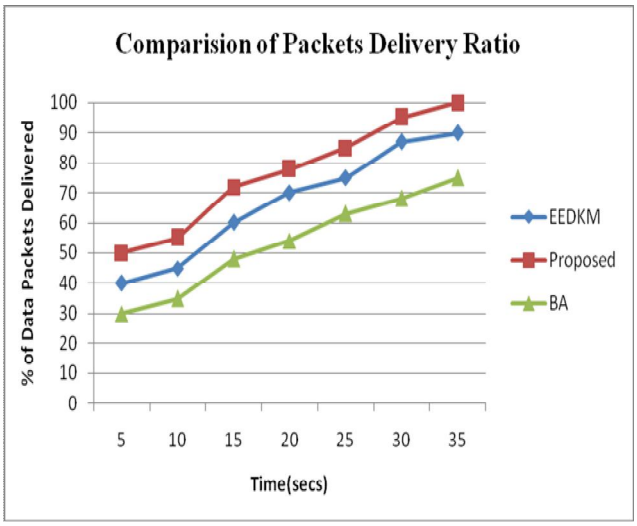

Figure 15 – Performance comparison of PDR

As shown in the above figure, the horizontal axis represents packet rate while the vertical axis represents the number of packets delivered. The results revealed that packet delivery increases as packet rate increases. The proposed scheme shows better performance when compare to other schemes.

5. DISCUSSION

Recently Ghasemzadeh et al. [21] proposed PKC-based key agreement protocol that consumes less energy in WSN besides providing high level of security. In our previous paper [2] we explore a dynamic key management scheme for WSN. We used cluster-based sensor network for implementing key management scheme. PKC is used for the proposed key management scheme which is based on broadcast authentication. The proposed scheme could efficiently handle attacks launched by adversaries besides ensuring that dead nodes cannot cause security leaks. The proposed scheme was energy efficient and can also handle compromised cluster head efficiently. Simulation results reveal that the proposed scheme is energy efficient and supports dynamic key management in dynamic network environment for high level of security. Compared with BA scheme, our scheme in [2] improved performance of WSN significantly in terms of energy efficiency (Figure 5 of [2]).

Then we improved our scheme in this paper to make it robust to various attacks like black hole, carousel, rushing, wormhole, Sybil and flooding attack. Extensive simulations reveal that the proposed approach is capable of preventing such attacks in WSN. When compared with our existing solution the enhanced scheme shows significant performance improvement in terms of throughput by 66.6%, energy efficiency by 70%, delay performance by 12.5%, packet dropping by 16% and packet delivery ratio by 25% besides attack resiliency. Our work in this paper is compared with our previous paper [2]. The results revealed that this paper has made significant performance improvement in terms of energy consumption (Figure 7 of [2]), throughput (Figure 8 of [2]), packet dropping (Figure 9 of [2]), delay performance (Figure 10 of [2]) and packet delivery ratio (Figure 11 of [2]).

6. CONCLUSIONS AND FUTURE WORK

In this paper we studied various attacks on WSN such as black hole attack, carousel attack, rushing attack, wormhole attack, Sybil attack and flood attack. The attack model and defence mechanisms are proposed and implemented in the key management scheme proposed by us earlier [2]. The scheme is dynamic key management for dynamic WSN. It was proved to be energy efficient. In this paper our scheme is enhanced to throw light into the attack models and prevention mechanisms. The WSN used for experiments is cluster based with three layers such as base station, cluster header and sensor node. Security and energy efficiency are the two primary objectives of the scheme. In this paper it shows resiliency to the aforementioned attacks. Extensive simulation study results revealed that our scheme is dynamic and can be used with dynamic WSN for safeguarding its communications. Our scheme is compared with existing solutions and found to be better in terms of packet delivery ratio, energy consumption, delay performance, throughput and dropping. Besides, the scheme is robust to various

attacks launched by adversaries. This research can be extended further to explore the trade-off dynamics between level of security and the computational and communication overhead in dynamic WSN.

References

[1]. C.Krishna Priya and B.Satyanarayana. (2014). A REVIEW ON EFFICIENT KEY MANAGEMENT SCHEMES FOR SECURE ROUTING IN MOBILE AD HOC NETWORKS. ijcea, p-13-24.

[2]. C.Krishna Priya and Bachala Sathyanarayana. (2015). Energy Efficient and Dynamic Key Management Scheme for Wireless Sensor Networks.IJAIEM. 4, p-105-115.

[3]. Gulshan Kumar, Mritunjay Rai and Gang-soo Lee "Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement" International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012.

[4]. Madhavi, S. and K. Duraiswamy. (2013). FLOODING ATTACK AWARE SECURE AODV. Journal of Computer Scienc. 9 (1), p.1-9.

[5]. Jiejun Kong, Xiaoyan Hong, Mario Gerla, "A new set of passive routing attacks in mobile ad hoc networks—,This work is funded by MINUTEMAN project and related STTR project of Office of Naval Research, p1- 6.

[6]. Eugene Y. Vasserman and Nicholas Hopper. (2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. IEEE. 12 (2), p.32-44.

[7]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. (2002). Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. ACM SIGSOFT Software Engineering Notes, p.1-9.

[8]. E. A .Mary Anita,V. Vasudevan. (2010). Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining. International Journal of Computer Applications. 1 (12), p.2001-2015.

[9]. Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil. (2004). Black Hole Attack Injection in Ad hoc Networks. Computational Sciences and Engineering Division. n. p.450-550.

[10]. Monika Roopak , Dr. Bvr Reddy. (2011). Performance Analysis of Aodv Protocol under Black Hole Attack. International Journal of Scientific & Engineering Researc. 2 (8), p.345-440.

[11]. Madhavi, S. and K. Duraiswamy. (2013). FLOODING ATTACK AWARE SECURE AODV. Journal of Computer Scienc. 9 (1), p.1-9.

[12]. Siddhartha Choubey1, Abha Choubey2 , M.Abhilash3 , Kamal K Mehta4. (2005). Defense Mechanisms against Hello Flood Attack in Wireless Sensor Network. wsn, p.123-135.

[13]. Khushboo Sawant, Dr. M.K Rawat. (2014). Survey of DOS Flooding Attacks over MANET Environment. Khushboo Sawant et al Int. Journal of Engineering Research and Applications. 4 (5), p.450-550.

[14]. V. PALANISAMY, P.ANNADURAI2. (2009). Impact of Rushing attack on Multicast in Mobile Ad Hoc Network. (IJCSIS) International Journal of Computer Science and Information Security. 4 (1), p.1-9.

[15]. Chinkit Suthar, Bakul Panchal. (2014). Rushing Attack Prevention with modified AODV in Mobile Ad hoc Network. 2014 IJEDR. 2 (4), p.234-305.

[16]. Eugene Y. Vasserman and Nicholas Hopper. (2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. IEEE. 12 (2), p.32-44.

[17]. Hyunsung Kim. (2014). End-to-End Authentication Protocols for Personal/Portable Devices over Cognitive Radio Networks.International Journal of Security and Its Applications. 8 (4), p.123-135.

[18]. S.Manimala, A.Taskala Devapriya. (2014). Detection of Vampre Attack Using EWMA in Wireless Ad Hoc Sensor Networks. IJISET - International Journal of Innovative Science, Engineering & Technology. 1 (3), p.450-550.

[19]. Qinghua Zhang, Pan Wang, Douglas S. Reeves and Peng Ning. (n.d). Defending against Sybil Attacks in Sensor Networks. (n.d), p1-7.

[20]. L. Lazos, R. Poovendran, C. Meadows, P. Syverson and L. W. Chang. (n.d). Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach (n.d), p1-7.

[21]. Hamzeh Ghasemzadeh, Mohammad Reza Aref, Ali Payandeh (2000). A novel and low-energy PKC-based key agreement protocol for WSNs adversary. Broadcast Authentication. IEEE, p1-7.

AUTHORS

Prof. B.Sathyanarayana received his B.Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985, Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri Krishnadevaraya University, Anantapuramu, A.P. India. He has 24 years of teaching experience. His Current Research interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals

C.Krishna Priya received her Master of Computer Applications from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007, MTech (IT) from Karnataka State Open University , Mysore , Karnataka in 2011. She is currently pursuing her Ph.D in Computer Science and Technology at Sri Krishnadevaraya University, Anantapuramu, A.P., India. Her current research interest includes Computer Networks