Outlier Detection and Treatment for Lightweight Mobile Ad Hoc Networks

Adarsh Kumar[1,2], Krishna Gopal[2], and Alok Aggarwal[1,3]

[1] Computer Science Engineering and Information Technology Department,
[2] Jaypee Institute Of Information Technology, Noida, India
[3] JP Institute Of Engineering and Technology, Meerut, India
{adarsh.kumar,krishna.gopal}@jiit.ac.in, alok289@yahoo.com

Abstract. This work is to detect and prevent unprecedented data identified from lightweight resource constraint mobile sensor devices. In this work, event or error detection technique of Traag et. al., local-global outlier algorithm of Branch et. al., Teo and Tan's protocol of group key management and Cerpa et. al protocol of Frisbee construction are integrated and modified for lightweight resource constraint devices [20][22]-[24]. The proposed technique in this work is better than other techniques because of: (a) scalability, (b) optimization of resources, (c) energy efficient and (d) secure in terms of collision resistant, compression, backward and forward secrecy. The deviations in modified form of proposed mechanism are corrected using virtual programmable nodes and results show that proposed scheme work with zero probability of error and attack.

Keywords: lightweight, outlier, anomalies, security, key management, MANET.

1 Introduction

Mobile Ad Hoc Networks (MANETs) consist of self configuration, infrastructure less, short range wireless technology, dynamic topology and mobile or semi-mobile devices. Various applications of MANETs are: Vehicular Ad-Hoc Networks (VANETs), house-hold appliances, military purposes, commercial security devices, peer to peer applications, mobile game programming etc. Major challenges of these types of networks are: security constraints, scarcity of resources, limited bandwidth availability, small subnets, traffic overhead, high processing cost etc. Since MANETs frequently and dynamically changes subnets thus these low capacity devices demand lightweight or ultra lightweight cryptographic implementation. According to Moore's law, only 30% resources are available for cryptographic primitives. Various security primitives need to be integrated within available resources for resource constraint mobile nodes are [1]:

- Availability: ensures that nodes should be available for communication despite of any worst conditions.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 750–763, 2013.

- Confidentiality: ensures the security breach of information during communication should not be compensated at any cost.
- Integrity: guarantees that message or user authentication information is never corrupted.
- Authentication: ensures that impersonation, masquerading and interference of resources, user identities and sensitive information should not be tolerated.
- Authorization: ensures that resource or information is trusted and collision resistant.
- Key Management: promises that key generation, transportation, confirmation and renewing is proper, secure and fast.
- Non-repudiation: convince the source node from not betray from sending information and other nodes about compromised source node.

Other security factors that need to be taken care of are: frequent key contributiveness, pre-image resistant, information distortion, message replay, active or passive attacks etc. This work is in continuation of work done to secure the MANET with respect to confidentiality, integrity, authentication & authorization and key management for resource constraint devices [23]. In this work, concentration is drawn towards availability of nodes for communication despite of attacks or corruption. Intrusion is an important security breach and is meant to compromise the cryptographic primitives like: availability, confidentiality, integrity, key management. Non-availability of nodes is mainly due to outliers or anomalies created inside the network [2]. The outliers or anomalies are the deviations of data as compared to normal data in order to gain some advantage.

The rest of the paper is organized as follows. Section 2 provides introduction to anomalies and classification of various outlier detection techniques. Section 3 describes the proposed approach to distinguish between an error or an event based on Markov chain and proposed local-global outlier detection algorithm. Section 4 describes the experimental setup, performance analysis of proposed algorithm, verification and validation of results and algorithm correction. Section 5 presents the conclusion.

2 Related Work

2.1 Outliers in Sensor Based Networks

Various sources of outlier in sensor networks are: (a) Fault detection, due to hardware, software or environmental anomalies [3-4], (b) automatic event detection, due to uncertainty in data [5-6], [11-12] and (c) intrusion detection, due to deviation from regular system usage in order to compromise security primitives [7-9]. These anomalies can occur at data, node or network levels [10].

2.2 Outlier Detection Techniques

In the literature, outlier detection techniques can be classified into various categories:

First classification is based on node, network or data based outliers. Node based outliers occur from internal system calls with sequential data [13]. Network based outliers occur from network generated socket calls and data based outliers are because

of calculation errors. Various node, network and data level detection techniques are: statistical techniques based methods, models based methods, state machine based methods, neural network based, rule based systems etc.

Second classification is based on: (a) data attributes and its correlation, (b) local or global views of outliers, (c) error, event or attack based outliers, (d) degree of deviation from normal data and (e) supervised, semi-supervised or unsupervised data. Various detection techniques used to analyze outliers based on above classification can be categorized as: (a) statistical based techniques, (b) nearest neighbor based, (c) clustering based, (d) bayesian network based, (e) spectral decomposition based etc. Statistical based techniques can have the knowledge about data. For example, Gaussian based techniques. Statistical techniques without prior data information are: kernel based or histogram based [14]. Well known nearest neighbor based technique is single hop Frisbee construction technique [24].Other non-statistical techniques are: network intrusion detection, neural network based etc.

Third classification is based on supervised or unsupervised detection mode. Supervised data techniques have prior knowledge about data sets consisting of information about anomalies and normal data. Unsupervised techniques do not have any prior information about data sets. For example, supervised techniques are: Bayesian network based, SVM based and unsupervised techniques are: statistical based, knowledge based, neural network based, fuzzy logic based, Markov or Hidden Markov Model (HMM) based, nearest neighbor based, clustering algorithm based etc [15][16][30].

Fourth classification is based on: (a) distance based, (b) density based, (c) machine learning or soft computing based. Distance based outlier detection are based on distance between selective node's attributes from the data set taken into consideration. For example, Hawkin outlier [17] and DB outlier technique [18]. Popular density based outlier techniques are: LOF, RDF, natural outlier based etc [31]-[33] and machine learning based technique is: SVM.

Fifth classification is based on: (a) local outlier, (b) global outliers, (c) semi global outliers, (d) distributed global outliers and (e) semi-global distributed outlier detection mechanism. In these outlier detection techniques local views of neighbors are collected to form a local view and then these views are further broadcasted to global nodes [20].

In this work, hybrid approach is developed for lightweight devices. Lightweight protocol are identified and integrated in order to get energy efficient, optimized and scalable solution for resources constraint mobile sensor devices. First an approach of distinguishing between an event and an error for a mobile node is proposed using Markov chain, which is based on Traag et. al. technique [25]. A lightweight local-global outlier detection mechanism is integrated with modified Teo and Tan's protocol for anomaly score calculation [20]. In order to validate the results, automated security tools are studied and two tools are used for experimental evaluation [34].

3 Proposed Approach

3.1 Assumptions and Premises

Let 'R' be the region selected for observation at starting time T_S to ending time T_E during a week of observation w_o. Let T_{WIN} is the time window $[T_S, T_E]$ of a complex

event. T_{WIN}^{o} be time window during week 1 to W. Furthermore, a node made message communication or acting as router 'ROU'. Let node has started message communication MC_1…….MC_n during time TC_1….TC_n and routing ROU_1^M…… ROU_n^M at time $TROU_1$….$TROU_n$ in time window T_{WIN}. $MOBC_1^{((x_1^i,y_1^i)\ldots\ldots(x_1^n,y_1^n)}$ … … …. $MOBC_1^{((x_1^i,y_1^i)\ldots\ldots(x_1^n,y_1^n)}$ be the mobility of nodes during message communication and $MOBROU_1^{((x_1^i,y_1^i)\ldots\ldots(x_1^n,y_1^n))}$ … … …. $MOBROU_1^{((x_1^i,y_1^i)\ldots\ldots(x_1^n,y_1^n))}$ be the mobility of nodes during routing. Following are the steps to be followed in order to calculate anomaly score.

1. *Find the probability that a mobile node is following a particular path.*

Let $P_{(i,\ j)}$ be the probability of any mobile node MN_x to move from $MN_z^{(x_i,y_i)}$ *to* $MN_z^{(x_z,y_z)}$, where z∈[1…n].

According to Markov chain, a probability of following a path through states $s_1^{(x_1,y_1)}$ to $s_n^{(x_n,y_n)}$ is calculated as:

$P(s_1^{(x_1,y_1)}, s_1^{(x_2,y_2)} \ldots\ldots\ s_n^{(x_n,y_n)}) = s_1^{(x_1,y_1)}, s_1^{(x_2,y_2)} \ldots\ldots\ s_n^{(x_n,y_n)} = P(s_1^{(x_1,y_1)} = s_1^{(x_1,y_1)}) p_{x_1x_2} p_{x_2x_3} \ldots\ldots p_{x_{n-1}x_n} = P_S$

With integration of communication states and routing states, probability can be calculated as:

$P_S = P((S_{MOBC_1}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))} || S_{MOBROU_1}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))}), \ldots\ldots\ldots\ldots (S_{MOBC_n}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))} || S_{MOBROU_n}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))}) = P(s_1^{(x_1,y_1)} = (S_{MOBC_1}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))} || S_{MOBROU_1}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))}))\ p_{x_1x_2} p_{x_2x_3} \ldots p_{x_{n-1}x_n}.$

2. *Find the probability that node is attending regular event in a region 'R'.*

In order to find this probability, average probability of presence in a regular region 'R' by mobile node 'MN' using T_{WIN} is calculated as:

$$P_S^{AVG} = (1/(W-1)) \sum_{v=1, v=w}^{W} P_s(MN, R, T_{WIN}^v)$$

According to Markov chain, every next sequence is dependent upon previous states. Thus

$$P_S^{AVG} = \left(\frac{1}{W-1}\right)\left(\sum_{v=1, v=w}^{W} (S_{MOBC_1}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))} || S_{MOBROU_1}^{((x_1^i,y_1^i)\ldots\ldots((x_1^n,y_1^n))}) \right.$$
$$\left. . p_{x_1x_2} p_{x_2x_3} \ldots p_{x_{n-1}x_n}, R, (T_{WIN}^{T_S} \ldots\ldots\ldots T_{WIN}^{T_S})_v \right)$$

3. *Detecting an event*

In order to find that whether an event has occurred or not, anomaly score is calculated as:

Anomaly Score = ($MN_{Active}^{Attendee}$ - ($AVG_{(MN_{ACTIVE}+MN_{SLEEP})}^{Attendee}$)) / STDEV

Higher event range values than threshold (>4) are considered as anomalies.

3.2 Distributed Local-Global Outlier Detection Mechanism

After deciding the method to distinguish between an event and an error in subsection 3.1, strategy of how to deploy detection method is proposed in this subsection. Detection methods can be deployed (a) centrally or (b) distributed. In centralized outlier detection deployment, it is required to collect all data at one central node and test it by single or group of nodes. Such a centralized mechanism has several disadvantages [19]: (a) expose central point of failure for system, (b) data collection and processing at some central point can cause end to end delays, (c) power consumption overhead on centralized and intermediate nodes, (d) scalability and robustness of network make it imperative to deploy the strategy distributed.

3.2.1 Distributed System Setup

The distributed system architecture consists of local view formation and global view formation strategies. In local view formation, a group of nodes in close vicinity form the view about anomaly in the data sets. These views collectively help in formation of weighted score for global view formation. Global view will instruct the active nearby nodes of Markov chain trajectory's sensor nodes to update anomaly score. Based on this anomaly score, the misbehaving nodes $\sum_{i=1}^{n} MN_i$ are charged for power and communication loss until they prove their authenticity. Neighboring nodes will change the view about a particular node MN_i if k-neighboring nodes agree to authenticate the node MN_i. The factor 'k' is calculated using distributed algorithm [20] and Shamir's threshold secret sharing scheme [21].

As shown in figure 1, in order to deploy distributed approach J. C. M. Teo and C. H. Tan's approach of group formation is modified for mobile nodes[22][23]. Each subgroup will form a local view in terms of anomaly score and this anomaly score is transmitted to main group controller through subgroup controller during group key updating process. If some critical updating is required then it can initiate Critical Updating Process (CUP) prior to group key updating process. Examples of critical situations are: sensor malfunctioning due to tsunami or earthquake, power failure etc. Algorithm for CUP is discussed in next subsection. Top layer of hierarchy consist of single main group and every other subgroup is controlled by subgroup controller in its parent directory. Virtual nodes help in formation of optimized subgroups in close vicinity. Each subgroup runs an algorithm at its local level called Local View Formation algorithm (LVFA) and main group runs Global View Formation Algorithm (GVFA) for anomaly score calculation. These algorithms are described in next subsections.

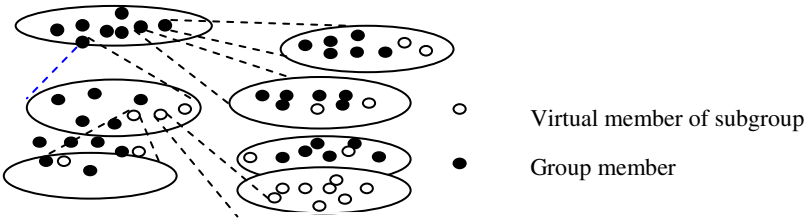

Fig. 1. Virtual group/subgroup hierarchy

3.2.2 Local View Formation algorithm

In this subsection, LVFA is proposed through which mobile sensor nodes in a subgroup form a generalized view about an event in a close vicinity. If anomaly score of an event increases a threshold limit then the error is reported to main group controller. In the process of error or anomaly formation, it should be taken into consideration that sensor nodes have scarcity of power resources and thus its losses should be minimized. In order to minimize the losses, "Frisbee Model" is integrated with Markov chain to trace the path of a mobile node and Frisbees [24]. These Frisbees will help to form a view about an event or calculate anomaly score at local and global levels. In order to implement optimal Frisbee, Teo and Tan's group key management protocol is used for secure message exchange and one hop nearest neighbor will construct the Frisbee periphery. Figure 2 shows the construction of Frisbees with integration of Teo and Tan's protocol of subgroup construction. Figure 2a shows the possible trajectory according to Markov chain. Figure 2b shows the construction of Frisbee periphery using single hop neighbor based shamir's threshold scheme. Figure 2c shows the sequence of Frisbees constructed during node's mobility or trajectory. LVFA is developed as follows:

Protocol: Local event or anomaly detection.

Premises: Let HL_i is the hierarchy of subgroups $SG_j^{HL_i}$, where each subgroup consists of 'n' number of elements and iϵ{1,2,3…..s}, jϵ{1.2…r}. 'h' is the height of hierarchical structure such that $m=n^h$, j^{th} subgroup at i^{th} layer for jϵ{0….. n^i-1} is represented by $SG_j^{HL_i}$, subgroup controller of j^{th} subgroup at hierarchical layer HL_i is represented by $SG_{SC_j}^{HL_i}$. k^{th} member of j^{th} subgroup at hierarchical layer HL_i is represented as $SM_{(j,k)}^{HL_i}$, where k=jn+l for lϵ{0,…..n-1}. Data compression, collision resistance, forward and backward secrecy is achieve through a hash function 'H'. $SMO_{(j,k)}^{HL_i}$ represents the outlier node in i^{th} hierarchy.

Goal: Form subgroups and calculate anomaly score.

Step 1: Form initial 1-hop nearest neighbor Frisbee

a. $SM_{(j,k)}^{HL_i}$ broadcasts it's group key updating request to other nodes in the subgroup $SG_{SC_j}^{HL_i}$.

b. Like $SM_{(j,k)}^{HL_i}$'s contribution request to update group key, all subgroup members will send their primitive contributions also.
c. $SG_{SC_j}^{HL_i}$ will decide the neighbor nodes of $SM_{(j,k)}^{HL_i}$ based on 1-hop criteria and form initial Frisbee.

Step 2: Apply Markov chain model & found the possible Frisbee trajectory.

a. Markov chain will give an approximation of trajectories to be followed by mobile node in order to attend an event using formula:
$P_S = P(s_1^{(x_1,y_1)} = s_1^{(x_1,y_1)}) p_{x_1x_2} p_{x_2x_3} \cdots\cdots p_{x_{n-1}x_n}$
The best path is selected (i.e. $P_S = 1$).
b. $SG_{SC_j}^{HL_i}$ calculate anomaly score based on scheme mentioned in subsection 3.1 and update $SG_{SC_j}^{HL_{i+1}}$ with anomaly score and trajectory followed in j[th] subgroup at i[th] layer.

Step 3: Outlier node can later put a request to nearby nodes for change of their views based on new anomaly score.

a. If some $SM_{(j,k)}^{HL_i}$ is found as sending data anomaly source then using previous two steps, it can be easily detected.
b. After some time interval, if same mobile node $SM_{(j,k)}^{HL_i}$ want to attend an event then it will send a request to it's subgroup controller.
c. $SG_{SC_j}^{HL_i}$ will use Burmester & Demesdt protocol (BD protocol) to prove the authenticity and shamir's threshold mechanism to recalculate it's anomaly score [21][29].

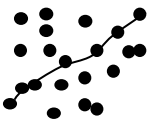

Fig. 2a. Possible trajectory using Markov model

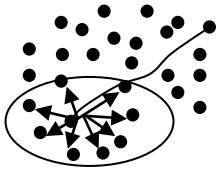

Fig. 2b. 1-hop nearest neighbor Frisbee formation

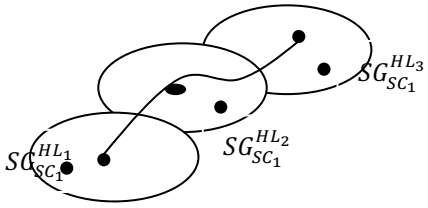

Fig. 2c. Sequence of Frisbees formed during trajectory

Fig. 2. Frisbee formation during LVFA

3.2.3 Global View Formation algorithm

Protocol: Global event or anomaly detection

Premises: Same as local event or anomaly detection protocol.

Goal: Collect anomaly scores from subgroups and broadcast opinion about outliers.

Step 1: Collecting anomaly scores from all layers.

a. $SG_{SC_j}^{HL_i}$ of each layer will send encrypted anomaly score to its parent subgroup controller.
b. This subgroup controller will send an integrated encrypted report to its parent subgroup controller.
c. This process will continue until all anomaly score are collected by primary subgroup controller.

Step 2: Form a global view of outlier nodes.

a. As outlier node can attend some other events in different subgroup thus a generalized option about outlier nodes should be communicated to each subgroup controller.
b. All outlier mobile nodes $SMO_{(j,k)}^{HL_i}$ are identified. A report of outliers is formed and sends to subgroup controllers. $SG_{SC_j}^{HL_i}$sends the report to every subgroup controller at HL_{i+1} layer.
c. At local level, views can be updated using same process as in LVFA's step 3.

3.2.4 CUP Algorithm

Protocol: Anomaly updating before renewing the group key.

Premises: Same as local event or anomaly detection protocol.

Goal: Collect anomaly scores from subgroups and broadcast opinion about outliers.

Step 1:- $SG_{SC_j}^{HL_i}$ sends E_K("Anomaly") to $SG_{SC_j}^{HL_{i-1}}$.

Step 2:- Step 1's process continues until it reaches to main subgroup.

Step 3:- Top layer hierarchy subgroup controller $SG_{SC_j}^{HL_i}$initiate the process of group key formation.

Strengths of proposed mechanism are: (a) solution is optimized and scalable, (b) work with integration of lightweight encryption/decryption process, (c) energy efficient because of Frisbee model, (d) provide security from well known attacks.

4 Result and Analysis

4.1 Experimental Setup

In order to evaluate the performance, Linux operating system is selected with ns-3 platform and python language [26]. Number of nodes selected for analysis varies from 50 to 200. The parameters taken for analysis are: anomaly detection ratio (ADR),

wrongly calculated anomaly ratio (WCAR), average local anomaly detection ratio (ALADR) and average local wrongly calculated anomaly ratio (ALWCAR). ADR is the ratio of anomalies detected by local-global mechanism to original number of anomalies present in the data set. WCAR is the ratio of number of normal data detected as outlier to total number of anomalies. ALADR & ALWCAR are the average values of local subgroup's ADR and WCAR respectively.

Table 1. Different detection ratios to calculate success rate

	N=50	N=100	N=200
ADR	0.860	0.770	0.700
WCAR	0.010	0.060	0.090
ALADR	0.910	0.800	0.740
ALWCAR	0.001	0.009	0.011

Table 1 shows the analysis of various ratios. It can be seen that accuracy decreases with increase in number of nodes. Second, it is important to notice that the global outlier detection ratio is having errors. It means that global outliers are not getting scores properly. In order to correct the result following correction is made to local outlier detection algorithm.

4.2 LVFA Correction

In order to reduce the error at global level, LVFA is modified. After making this modification and result analysis, it is observed that this error was because of inactiveness of mobile nodes. In order to remove the error because of inactiveness, virtual node concept is added. Instead of storing local view about anomaly score at subgroup controller, it is stored at virtual node subgroup controller. These virtual nodes are the programmable nodes without any hardware as discussed in figure 1. The correction is as follows:

Protocol: Local event or anomaly detection.
Premises: Same as local event or anomaly detection protocol.
Goal: Remove the deviation using virtual programmable nodes.
Step 1: Same as Step 1 of local event or anomaly detection protocol.
Step 2: Apply Markov chain model & found the possible Frisbee trajectory.

a. Same as Step 2a of local event or anomaly detection protocol.
b. $SG_{SC_j}^{HL_i}$ calculate anomaly score based on scheme mentioned in subsection 3.1 and update $SG_{SC_j}^{HL_{i+1}}$ with anomaly score and trajectory followed in jth subgroup at ith layer.
c. $SG_{SC_j}^{HL_i}$ will send its information to virtual node subgroup controller $VNSG_{SC_j}^{HL_i}$. Like $SG_{SC_j}^{HL_i}$, $VNSG_{SC_j}^{HL_i}$operate and exchange information about subgroup. The main advantage of these virtual nodes is that these are supposed to be active throughout lifecycle.

Step 3: Outlier node can later put a request to nearby nodes for change of their views based on new anomaly score.

a. If some $SM_{(j,k)}^{HL_i}$ is found as sending data anomaly source then using previous two steps, it can be easily detected.
b. After some time interval, if same mobile node $SM_{(j,k)}^{HL_i}$ want to attend an event then it will send a request to it's subgroup controller.
c. $SG_{SC_j}^{HL_i}$ will use BD protocol to prove the authenticity and shamir's threshold mechanism to recalculate it's anomaly score.
d. $SG_{SC_j}^{HL_i}$ send calculated anomaly score to $VNSG_{SC_j}^{HL_i}$. These virtual nodes further exchange information about top layer virtual subgroup controller for calculation of global anomaly score.

4.3 Results Evaluation

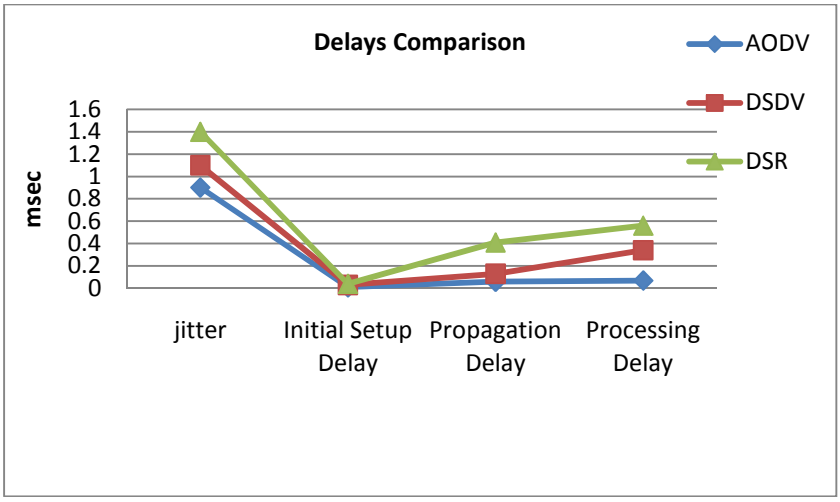

Fig. 3. Delay Comparison of proposed mechanism over MANET routing protocols

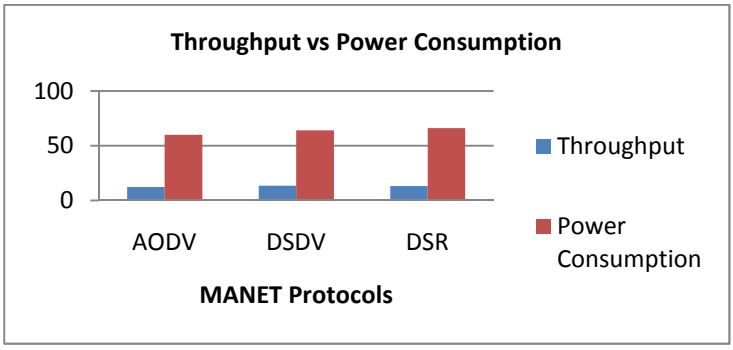

Fig. 4. Power vs Throughput comparison over MANET routing protocols

After making LVFA correction, it is found that error or deviation is negligible. Further, in order to evaluate the performance various parameters taken into the considerations are: end to end delay, throughput, jitter and power consumption. Figure 3 and Figure 4 shows that Ad On-demand Distance Vector (AODV) routing protocol is having minimum average value of end to end delay, jiiter, power consumption as compared to Dynamic Source Routing (DSR) and Destination Sequenced Distance Vector (DSDV) routing protocols. Since proposed protocol is also an on-demand protocol thus it resembles with the operations of AODV routing protocols and provide good amount of throughput. AODV and DSR are reactive routing protocols. Out of these two protocols, DSR is providing continuous increase in end to end delay than AODV because in proposed scheme single hop neighbor discovery protocol is used which is similar to the scheme used in AODV.

4.4 Verification and Validation

Process:

[Process]

--- Query [Query]

Completing……

Starting query [Query]

Goal [un] reachable: [Goal]

Abbreviations:

…….

…….

[Attack derivation]

…….

RESULT not attacker(secret SG N_{SG} []) is true

RESULT not attacker(secret SM N_{SM} []) is true

RESULT not attacker(secret SMO N_{SMO} []) is true

RESULT not attacker(secret VNSG N_{VNSG} []) is true

RESULT inj –event (endHL_iparam(x_1400)) ===> inj-event (beginHL_i(x_1400)) is true

RESULT inj –event (endSM_iparam(x_1589)) ===> inj-event (beginSM_i(x_1589)) is true

RESULT inj –event (endSG_iparam(x_1623)) ===> inj-event (beginSG_i(x_1623)) is true

RESULT inj –event (endSMO_iparam(x_1801)) ===> inj-event (begin SMO_i(x_1801)) is true

RESULT inj –event (endSMO_iparam(x_1945)) ===> inj-event (begin SMO_i(x_1945)) is true

Fig. 5. ProvVerif results showing passing of all tests

In this subsection, automated verification tools AVISPA and ProVerif are used to verify that protocol is protected from attacks or corruption [27][28]. These tools are used to graphically test various points of protocol failure under the inspection of different probability models. AVISPA check the security of protocols using HLPSL specification language. After checking against man in the middle, replay and denial of service attacks, it is found that tests have given "no attacks found" results. This validates that local and global outlier mechanism is secure. Figure 5 shows the results of proposed mechanism using ProVerif. ProVerif is used to test the backward and forward compatibility. Here backward compatibility means previous key will not help the attacker to find new key for any node. Here, if some attacker is able to find the key then it can easily manipulate the messages. Those messages will be considered as anomalies. Similarly, forward compatibility means if new key or keys are leaked then past key should be secure. This process can again generate anomaly data by an attack. Results show that protocol is secured from both backward and forward corruption.

5 Conclusion

In this work, Traag et. al., Branch et. al., Teo and Tan and Cerpa et. al. protocols of event detection in mobile phones, local-global algorithm for anomaly view formation, group key management and Frisbee construction protocols respectively are integrated and modified for lightweight resource constraint devices. After observing the error of 3 to 5 % in anomaly detection, correction to LVFA is made and result are verified using two automated verification and validation tools: AVISPA and Proverif. Results shows that proposed mechanism work efficiently with AODV routing protocol and with no attack.

References

1. Zhou, L., Haas, Z.J.: Securing Ad Hoc Networks. IEEE Network 13(6), 24–30 (1999)
2. Heady, R., Luger, G., Maccabe, A., Servilla, M.: The architecture of a network level instrusion detection system, Computer Science Department, University of New Mexico. Tech. Rep. (1990)
3. Chen, J., Kher, S., Somani, A.: Distributed fault detection of wireless sensor networks. In: Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, pp. 65–72 (2006)
4. Luo, X., Dong, M., Huang, Y.: On distributed fault tolerant detection in wireless sensor networks. IEEE Transactions on computers 55(1), 58–70 (2006)
5. Krishnamachari, B., Iyengar, S.: Distributed Bayesian algorithms for fault tolerant event region detection in wireless sensor networks. IEEE Transactions on Computers 53(3), 241–250 (2004)
6. Martincic, F., Schwiebert, L.: Distributed event detection in sensor networks. In: Proceedings of Systems and Network Communication, pp. 43–48 (2006)
7. Ding, M., Chen, D., Xing, K., Cheng, X.: Localized fault tolerant event boundary detection in sensor networks. In: Proceesings of IEEE Conference of Computer and Communications Socities, pp. 902–913 (March 2005)

8. Silva, A.P.R., Martins, M.H.T., Rocha, B.P.S., Loureiro, A.A.F.: Decentralized intrusion detection in wireless sensor networks. In: Proceedings of the 1st ACM international Workshop on Quality of Service and Security in Wireless and Mobile Networks, pp. 16–23 (2005)
9. Bhuse, V., Gupta, A.: Anomaly intrusion detection in wireless sensor networks. Journal of High Speed Networks 15(1), 33–51 (2006)
10. Jurdak, R., Wang, X.R., Obst, O., Valencia, P.: Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies. In: Tolk, A., Jain, L.C. (eds.) Intelligence-Based Systems Engineering. ISRL, vol. 10, pp. 309–325. Springer, Heidelberg (2011)
11. Buxton, H.: Learning and understanding dynamic scene activity: A review. Image and Vision Computing 21, 125–136 (2003)
12. Hu, W., Tan, T., Wang, L., Maybank, S.: A survey on visual surveillance of object motion and behaviors. IEEE Trans. Syst. Man Cybern., Appl. Rev. 34(3), 334–352 (2004)
13. Chandola, V., Banerjee, A., Kumar, V.: Outlier Detection: A Survey. ACM Computing Surveys, 1–72 (2009)
14. Zhang, Y., Meratnia, N., Havinga, P.: Outlier Detection Techniques for Wireless Sensor Networks: A Survey. IEEE Communication Surveys & Tutorials 12(2) (2010)
15. Gogoi, P., Borah, B., Bhattacharyya, D.K.: Anomaly Detection Analysis of Intrusion Data using Supervised and Unsupervised Approach. Journal of Convergence Information Technology 5(1) (February 2010)
16. Gogoi, P., Bhattacharyya, D.K., Borah, B., Kalita, J.K.: A Survey of Outlier Detection Methods in Network Anomaly Identification. The Computer Journal 54(4), 570–588 (2011)
17. Hawkins, D.M.: Ident fication of outliers. Chapman and Hall, London (1980)
18. Knorr, E.M., Ng, R.T.: Algorithm for mining distance based outliers in large datasets. In: Proceedings of the 24th International Conference on Very Large Databases, New York, USA, pp. 392–403. Morgan Kaufmann (1998)
19. Karl, H., Willig, A.: Protocols and Architectures for Wireless Sensor Networks. John Wiley & Sons (2007)
20. Branch, J.W., Giannelia, C., Szymanski, B., Wolff, R., Kargupta, H.: In-Network Outlier Detection in Wireless Sensor Networks. Knowledge and Information Systems 31 (2012)
21. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
22. Teo, J.C.M., Tan, C.H.: Energy-Efficient and Scalable Group Key Agreement for Large Ad Hoc Networks. In: PE-WASUN's 2005, October 10-13, pp. 114–121 (2005)
23. Kumar, A., Aggarwal, A.: Efficient Hierarchical Threshold Symmetric Group Key Management Protocol for Mobile Ad Hoc Networks. In: IC3, pp. 335–346 (2012)
24. Cerpa, A., Elson, J., Estrin, D., Girod, L., Hamilton, M., Zhao, J.: Habitat Monitoring: Application Driver for Wireless Communication Technology. In: Proceedings of the ACM SIGCOMM Workshop on Data Communication in Latin America and the Caribbean, San Jose, Costa Rica (2001)
25. Traag, V.A., Browet, A., Calabrese, F., Morlot, F.: Social Event Detection in Massive Mobile Phone Data Using Probabilistic Location Inference. In: Traag, V.A., Browet, A., Calabrese, F., Morlot, F. (eds.) SocialCom/PASSAT, October 9-11, pp. 625–628 (2011)
26. NS3 Simulator, `http://www.nsnam.org`
27. AVISPA toolkit, `http://www.avispa-project.org`
28. ProVerif protocol verifier toolkit, `http://www.proverif.ens.fr`
29. Burmester, M., Desmedt, Y.G.: A secure and efficient conference key distribution system. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 275–286. Springer, Heidelberg (1995)

30. Yang, J., Wang, Y.: A New Outlier Detection Algorithms based on Markov chain. Advanced Materials Research 366, 456–459 (2012)
31. Breunig, M.M., Kriegel, H.P., Ng, R.T., Sander, J.: LOF: Identifying Density Based Local Outliers. In: Proceedings of the ACM SIGMOD Conference, Dallas, TX (May 2000)
32. Wang, B., Perrizo, W.: RDF: a density-based outlier detection method using vertical data representation. In: IEEE Int. Conference on Data Mining, pp. 503–506 (2004)
33. Rajagopalan, S., Karwoski, R., Bartholmai, B., Robb, R.: Quantitative image analytics for strtified pulmonary medicine. In: IEEE Int. Symposium on Biomedical Imaging (ISBI), pp. 1779–1782 (2012)
34. Cheminod, M., Bertolotti, I.C., Durante, L., Sisto, R., Valenzano, A.: Tools for cryptograhic protocols analysis: A technical and experimental comparison. Journal on Computer Standards & Interfaces 31(5), 954–961 (2009)