International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Improved Outlier Detection Mechanism for Hierarchical Key Management in Hierarchical Mobile Ad-hoc Networks (MANETs)

Neeraj Chugh, Saurabh Jain, Adarsh Kumar, Alok Aggarwal, Neelu Jyoti Ahuja

Abstract*: The purpose of this paper is to present an outlier detection mechanism for hierarchical key management which utilizes hybrid (public and private) key management scheme for implementing lightweight cryptographic primitives in hierarchical MANETs. Further, a comparative analysis of key management schemes is to be performed for identifying an efficient key management scheme for hierarchical MANETs. In key management methods, public and private group key management schemes are integrated at local level (subgroup) and global level (network). These key management schemes uses various topologies for minimizing communicational and computational costs. After implementing an efficient key management scheme, outliers in network are identified using packet analysis at key generation, key distribution, message transmission and key re-generation phases. It is observed that Teo and Tan key management approach with shamir's threshold key distribution mechanism is an efficient approach key management scheme for group authentication and hierarchical key management. Further, a minimum improvement of 9.7% and 0.91%, and maximum improvements of 25.3% and 87.7% are observed for Packet Delivery Rate (APDR) and Average Throughput (AT) respectively in a network of 1000 nodes. The proposed method requires four sequential analysis of outlier detection schemes at different layers of MANET protocol stack because single scheme per layer is not efficient in identifying outliers in proposed network. The proposed key management method is useful for MANETs in group authentication and implementation of lightweight cryptographic primitives with secure key. Further, outlier detection mechanism can be extended for identifying various active and passive attacks.

***Keywords*: Outliers, Inliers, Attack detection, Density-based clustering, QoS.**

Manuscript published on 30 September 2019
* Correspondence Author
Neeraj Chugh*, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: nchugh.jain@ddn.upes.ac.in
Saurabh Jain, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: saurabh.jain@ddn.upes.ac.in
Adarsh Kumar, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: adarsh.kumar@ddn.upes.ac.in
Alok Aggarwal, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: alok.aggarwal@ddn.upes.ac.in
Neelu Jyoti Ahuja, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India. Email: neelu@ddn.upes.ac.in

I. INTRODUCTION

Lightweight cryptography is an efficient security solution to confined cluster based networks (like MANETs). In such networks, objects partner with each other through multi-hop routing and remote connectivity. In such dynamic networks, implementing security solutions is a major challenge. Security through lightweight cryptography start from key management. Key management involves key generation, key dispersing, key verification and key re-generation processes. Lightweight primitives and protocols are helpful in key management by providing security solutions to key administration in MANETs. In lightweight key management protocols, flexible clusters constituting nodes are accumulated temporarily with remote connections. This process gives a connected environment for subsequent processing. This environment is considered temporal because in dynamic nature of adhoc systems, constituting a connected trusted model is challenging. Thus, this is vital for an environment to start key management and distribution updated information to every cluster timely. Using these keys, clusters in MANET are protected from each other. In similar clusters environment, chances of attacks increases because anyone can constitute a new cluster and start fake relations with nearby clusters and afterward batter the MANET. There are many challenges in MANET like: dynamic topology, base foundation, node division among nearby clusters, communication through untrusted intermediate clusters, lack of nodes connectivity and consistency, low energy and resource constrained devices. These challenges increases the chance of attacks. As discussed earlier, key management consists of gathering required information, generate keys from collected information, distributing generated key to all clusters and nodes, and start re-generation process if any node leave or new node join clusters. Key management process using cryptography primitives helps in providing security to gathering information, secure key distribution and re-generation. For example, encrypted messages are generated when a node leaves the clusters as it has no right to get connected with old data as "Backward Secrecy". Among other challenges, key management involves nodes connectivity in tree formation, energy efficient process, packet failure rate, latency etc. In this work, three lightweight key management protocols are analyzed and extended for outlier detection. Three protocols are: Teo & Tan's [1][2], WLH [3][4], Tseng [5]-[7].

An outlier detection process is executed after data assumption, data computation, data storage and data post-storage stages. Four layer processing execute outlier detection after each stage followed by an aggregated process which take opinion of above four layers and give its outcomes. Simulation analysis shows nodes distribution, cluster formation and outlier detection process graphically.

Network performance is analyzed and it is observed that the proposed outlier detection scheme is efficient with WLH protocol. However, Teo & Tan protocol give better results with passage of time and increase in data rate and number of nodes. This paper is organized as follows. A survey on existing lightweight key management processes and appropriate outlier detection mechanisms is presented in section 2. In section 3, a novel outlier detection mechanism is proposed for key management process in hierarchical MANETs. Section 4 explains the simulation and performance analysis process for proposed outlier detection process in MANET with different number of nodes. Finally, section 5 concludes the work.

II. LITERATURE SURVEY

This section surveys various intrusion and attack detection mechanisms in wireless and mobile ad-hoc networks. These mechanisms are explained as follows:

Krontiris et *al.* [8] proposed a lightweight intrusion detection system named LIDeA. In this distributed system, nodes interact with their neighboring nodes and collaborate with them for identifying performance based intrusions. This scheme is useful and can be easily implemented over resource constrained devices. It saves number of communication steps, energy and memory.

Farhan et *al.* [9] investigated the problem of attack detection and tried to reduce the number of false positives in MANET. A cooperative intrusion detection system is proposed for false positive reduction. In this system, a hierarchical network is constructed for intrusion analysis. The hierarchical process investigates the nodes based on their performance. An agent based distributed system take advantage of hierarchical process in identifying attackers through intelligent, lightweight and smart solutions. The hierarchical process gives non overlapping zones for data gathering, applying data analytics and attack detection based on alert and alarm messages. This process reduces the number of data transmission steps and save the bandwidth which makes it suitable for resource constrained hierarchical MANETs. The proposed model is dynamic enough for incorporating changes to existing network from side channel analysis. This model can be extended for small scale to large scale networks.

Kumar and Dutta [10] surveyed various prominent intrusion detection techniques in MANETs differentiated with technology and detection process. The proposed survey classify intrusion detection techniques into nine categories. A comparative analysis of existing techniques is performance for future directions in design and implementation of attack detection systems. Various observations of this work are as follows:

- It is found that there is no globally accepted metric for assessing the efficiency of existing and upcoming detection systems. However, few researchers have considered attack detection latency and receiver's operating characteristics in evaluation but results and analysis can mislead or give incomplete observations in detection.
- Various performance indices like power and resource usage, computational and communicational overheads, processing load etc. are used by researchers for intrusion detection. In performance and efficiency, detection process is affect by network performance as well. For example, flooding packets increases false positive alarms to a large extant and deteriorate the intrusion detection efficiency. Further, if an attacker is able to identify the intrusion detection host then it can make the host busy and take control over detection activities. Thus, self-protection is primary step in detection process.
- Node profile is built and data is analyzed after gathering. Detection process in existing approaches relies on normal profile which may be misleading and affect the detection accuracy and efficiency. In dynamic networks like MANETs, it is challenging to distinguish between "normal profile" and "abnormal profile" as any attacker node can impersonate with normal profile.
- Detection can be offline or online. Offline detection is efficient in terms of energy consumption and detection but requires a large storage space and there are chances of data leakage if proper security aspects are not taken into consideration. Online detection processes are required to be lightweight for maximum performance and minimum resource consumption. Integration of lightweight cryptography primitives and protocols ensure data integrity, confidentiality and authentication. Lightweight processes reduce computational and communication delays as well.
- Intrusions are detected using data attributes extracted during data enrichment and analysis. Interrelationships among data attributes are identified for detection process. Dynamic changing relationships act as detection point and help to segregate regular and anomalous relations. These relationships build datasets useful for assessment of intrusions in MANETs.
- Attackers are aware that most of the detection processes operate at lower layer of MANET protocol stack whereas application layer activities are hardly observed. Thus, it is important to concentrate on application layer data and processes for outlier detection. Analysis at all layers should be self-managed and self-configured to monitor and control dynamic network so as to quickly adapt and identify intruders.
- Rule-based detection processes are suitable for large amount of data and gives high accuracy and real-time analysis. This type of system is helpful at lower layers of MANET protocol stack suitable for designing of parallel and distributed intrusion detection systems.

In conclusion, various approaches are existing for finding the solutions to detect intrusions in MANETs. Different approaches have different requirements and work efficiently with different data attributes.

Thus, single approach is not considered to be reliable for detecting all types of attacks or one type of attack with single set of attributes. In conclusion, an approach is required to be proposed for detecting attacks that works at multiple layers with multiple data attributes.

Zamil and Samarah [11] proposed data mining techniques useful for vehicular ad-hoc networks (VANETs). Research methodologies are discusses which apply data pre-processing, outlier identification, clustering and data analytics over classified data for attack detection. The proposed system work successfully for centralized, distributed, offline and online techniques. A comparative analysis of existing algorithms is performed which is helpful in predicting attacks in dynamic environments.

Uddin et *al.* [12] proposes Signature-based Multi-layered intrusion detection approach suitable to work efficiently for small and multiple databases. Here, mobile agents are used for data collection, analysis, prediction and evaluation. These agents are also helpful in identifying node patterns in intrusion processes. In experimental evaluation, it is observed that verification and validation processes used for analyzing large environments are suitable for intrusion detection with threshold based outlier process. In performance, it is observed that there is significant improvement in detection rate because there is significant drop in packet drop rate. The proposed model is helpful in attack detection with signature distribution across databases of multiple detection systems. Distributed signatures are helpful in identifying patterns and predicting anomalous pattern. A node is considered to be normal if similar signature and pattern is observed at different point. If similar patterns and signatures are observed beyond an upper threshold or below lower threshold then these nodes or their data attributes are considered under scruity.

III. PROPOSED APPROACH

In this section, a multilayered outlier detection mechanism is proposed for hierarchical key management in hierarchical MANETs. This process detects outliers in multiple layers. Figure 1 shows the proposed outlier detection multi-layered architecture. Overall, outlier detection process is divided into five layers consisting of outlier detection at key generation, distribution, re-generation and message sending stages. In addition, an aggregated outlier detection layer is added for observing all above layers and identifying most vulnerable nodes. Detail functionalities of each of these layers is explained in following subsections. In this work, three protocols are considered for analysis [1]: Teo & Tan's Protocol [2], WLH [3][4], Tseng [5]-[7]. These protocols are discussed in protocol 1, protocol 2 and protocol 3.

Protocol 1: Teo & Tan's Protocol
Goal: To compute and share a common group key among all members of a hierarchical network.

Step 1: Identify field for computation.
Step 2: Each node will generate random number for Burmester-Demdst Group Key Agreement (BD-GKA) protocol.
Step 3: Each node will select a hashing mechanism for key computation.
Step 4: Each node will compute key using exponentiation.
Step 5: In order to run BD GKA, each node will collect its key from predecessor and successor.
Step 6: Generate group key is encrypted using symmetric key encryption mechanism and distributed to other nodes.
Step 7: Root of hierarchical network collects keys for all of its child nodes and generate a common key.
Step 8: Root generates a common key and distribute it to all of its child nodes.
Step 9: Each node will compute its key and storage in its memory.
Step 10: Each node will receive common key from root through group head and store it in its memory.
Step 11: Each group head will keep-track of nodes joining or leaving groups.
Step 12: Once a node leave a subgroup, each node in the network will regenerate a random number, compute its key and send over to group head. Each group head will send its subgroup contribution to root node, and root node will generate and distribute new group key to all nodes.
Step 13: If a new node want to join any existing subgroup then that particular subgroup head will collect its contribution and initiate the key refreshment process as specified in step (ii).
Step 14: Each new key either computed or received by any node replaces existing key stored in memory.

Protocol 2: WLH Protocol
Goal: To compute and share a common group key among all members of a hierarchical network.

Step 1: A random number is selected in a given field.
Step 2: Node identification, secret key and random number are encrypted and distributed to other nodes.
Step 3: Other nodes decrypt this message and store the information in their database.
Step 4: All other nodes generates a random number and send it back to source.
Step 5: Source node generates the hash of encrypted message (generated in step 2) and send it to all other nodes.
Step 6: Hashed value is verified by all other nodes and consider it as session key.
Step 7: If there is need to re-generate key or start a new session then step 1 and step 2 are repeated initially.
Step 8: Random numbers are computed at all nodes except source node and a hash of previous encrypted user identification parameters and random numbers is computed. This hash value is considered as new temporary session key.

	Outlier Detection in Key Generation	Outlier Detection in Key Distribution	Outlier Detection in Message Sending (all types)	Outlier Detection in Key Re-generation	Aggregated Outlier Detection	Teo and Tan Protocol[2]	WLH Protocol [3][4]	Tseng Protocol [5]-[7]
Layer 1	Y				Y	Y	Y	Y
Layer 2		Y			Y	Y	Y	Y
Layer 3			Y		Y	Y	Y	Y
Layer 4				Y	Y	Y	Y	Y
Layer 5	Y	Y	Y	Y	Y			

Figure 1: Proposed Outlier Detection Multilayered Architecture

Step 9: A new hash value is computed from previous session key and session number.

Step 10: Random number and hash value is send over to source node for verification.

Step 11: Session number value is decreased and a new hash value is computed as final session key for new session. This key is computed at all sides separately.

Step 12: After generating the subgroup key using step 1 to 11, subgroup head send its group key to subgroup head of its parent subgroup and parent subgroup head send this key to its parent subgroup head. This process continues until all keys are received by root of hierarchical MANET.

Step 13: Root of the hierarchical network generates a common session key and distribute it to all nodes in the network. This key is used onward for message sending and other communications in the network.

Protocol 3: Tseng Protocol

Goal: To compute and share a common group key among all members of a hierarchical network.

Step 1: Each node generates a random number and computes exponentiation using generator of a field.

Step 2: Each node sends its contribution to subgroup head and subgroup head generates common key using a polynomial equation with input of contributions from all its subgroup members.

Step 3: Subgroup member broadcast its key to all its subgroup members.

Step 4: All subgroup members generate multiple polynomials for authentication and verification. These polynomials include: three hash values, one secret parameter, one exponentiation using generator and one exponentiation using message to send.

Step 5: Each node send these polynomials to subgroup head.

Step 6: Subgroup head computes inverse of all polynomials and verifies stored parameters. If all polynomials and stored parameters are verified then a random number is generated and send to all nodes.

Step 7: All nodes compute another parameters using hashing of received random number and common key (generated in step 3). This parameter acts as current session key.

Step 8: Subgroup head also generates session key at its own end. This key is same as all other node's keys.

Step 9: After generating the subgroup key using step 1 to 8, subgroup head send its group key to subgroup head of its parent subgroup and parent subgroup head send this key to its parent subgroup head. This process continues until all keys are received by root of hierarchical MANET.

Step 10: Root of the hierarchical network generates a common session key and distribute it to all nodes in the network. This key is used onward for message sending and other communications in the network.

The process of outlier detection starts from network construction and data collection. After data collection, data is refined for enrichment followed by multi-layered outlier detection. These steps are explained as follows:

a. Data Gathering

Simulation process is divided into multi-stages for data collection. These multi-stages are periodically run for key generation, distribution, re-generation and message sending. In data gathering phase, data is collection for analysis after each stage. In this data, each data element consist of source node, destination node, protocol used, flag bits, time, routing nodes etc.

b. Data Refinement

In this process, gathered data is analyzed for enrichment. Data enrichment process includes de-duplication, predicting missing entries, removing unwanted entries and predicting importance of data entries.

c. Layer-1 Outlier Processing

Table 1: Outlier Processing Division for Key Generation Process

	Teo & Tan	WLH Protocol	Tseng Protocol
Phase 1:- Data Assumption	Step 1, Step 2	Step 1, Step 2	Step 1
Phase 2:- Data Computation	Step 3, Step 4	Step 3, Step 4	Step 2
Phase 3:- Data Storage	Step 6	Step 4	Step 2

Table 2: Outlier Processing Division for Key Distribution Process

	Teo & Tan	WLH Protocol	Tseng Protocol
Phase 1:- Data Assumption	Step 5	Step 8	Step 4, Step 5

Phase 2:- Data Computation	**Step 10**	**Step 9**	**Step 6**
Phase 3:- Data Storage	**Step 11**	**Step 10**	**Step 9**
Phase 4:- Data Post-Storage	**Step 14**	**Step 12**	**Step 11**

Table 4: Outlier Processing Division for Key Re-Generation Process

	Teo & Tan	WLH Protocol	Tseng Protocol
Phase 1:- Data Assumption	After Step 14	Step 13	Step 10
Phase 2:- Data Computation	After Step 14	Step 13	Step 10
Phase 3:- Data Storage	After Step 14	After Step 13	After Step 10
Phase 4:- Data Post-Storage	After Step 14	After Step 13	After Step 10

At this stage, outliers are detected in key generation process. Key generation process varies from protocol to protocol. In order to identify outliers using single standardized process for all protocols, detection process is implemented at following common phases: data assumption, data computation, data storage and data post-storage stages. Table 1 shows the steps on or after which this layer's outlier detection is execute for four phases.

Table 3: Outlier Processing Division for Message Processing

	Teo & Tan	WLH Protocol	Tseng Protocol
Phase 1:- Data Assumption	After Step 11	After step 13	After step 8
Phase 2:- Data Computation	After Step 12	After step 13	After step 8
Phase 3:- Data Storage	After Step14	After step 13	After step 10
Phase 4:- Data Post-Storage	After Step 14	After step 13	After step 10

d. Layer-2 Outlier Processing

At this stage, outliers are detected in key distribution process. Like key generation, key distribution process also varies from protocol to protocol. In order to identify outliers using single standardized process for all protocols, detection process is implemented at following common phases: data assumption, data computation, data storage and data post-storage stages. Table 2 shows the steps on or after which this layer's outlier detection is execute for four phases.

e. Layer-3 Outlier Processing

At this stage, outliers are detected in message distribution. Like key generation and distribution process, message sending process also varies from protocol to protocol. In order to identify outliers using single standardized process for all protocols, detection process is implemented at following common phases: data assumption, data computation, data storage and data post-storage stages. Table 3 shows the steps on or after which this layer's outlier detection is execute for four phases.

f. Layer-4 Outlier Processing

At this stage, outliers are detected in key re-generation process. Like key generation, distribution process and message sending, key-regeneration process also varies from protocol to protocol. In order to identify outliers using single standardized process for all protocols, detection process is implemented at following common phases: data assumption, data computation, data storage and data post-storage stages. Table 4 shows the steps on or after which the outlier detection is execute for four phases.

g. Layer-5 Outlier Processing

Layer-5 outlier detection process is different from above four layer's processes. In this layer, user has the flexibility to either select outcome of any one of the above layer or apply proposed aggregated function for multi-layer outcome acceptance.

IV. Results and Analysis

In this section, simulation and results are analysed. In simulation a network is varies from 50 to 1000 nodes in a geographical region of 1000x1000 sq. meters. Packet data rate varies between 0.1 to 5 packets/second. Ray tracing radio propagation model is used for radio signal propagation. Network can have maximum packet size of 512 bits and each node can store a maximum of 50 packets in its queue. Nodes are mobile and it can vary between 0.3 m/s to 5 m/s. Figure 2 to figure 8 shows the visualization process of nodes distribution, cluster formation and outlier detection. Figure 2 shows nodes distribution at time 100 sec. and figure 3 shows cluster formation process after 100 sec. Similarly, figure 4 and figure 6 show nodes distribution after 200 and 500 sec. respectively. Their cluster formation are shown in figure 5 (after 200 sec.) and figure 7 (after 500 sec.). Figure 8 shows the outlier detection process after 1000 sec. Output of each layer is represented with different color. Red, blue, green, black and yellow color nodes are the outputs of outlier detection after layer-1, layer-2, layer-3, layer-4 and layer-5 processing respectively.

Figure 9 shows comparative analysis of throughput for lightweight key management protocols. In 150 nodes network, throughput is increasing with increase in time. Results show that WLH protocol provides higher throughput initially because of least computation but Teo & Tan's protocol throughput is higher with proposed process and with increase in time. Maximum percentage increase of throughput is observed in Teo & Tan protocol as compared to other protocols.

With increase in time, Tseng's protocol shows least throughput because of additional hashing function computations and encryption/decryption operations.

Figure 10 and figure 11 show comparative analysis of end-to-end delay for 75 and 150 nodes network. For 75 nodes network, delay is higher for Teo & Tan protocol, and least for Tseng's protocol with packet rate of 0.1 pkt/sec. As packet rate increases from 0.1 pkt/sec. to 5 pkt/sec., delay is reduced. With 5 pkt/sec., a minimum delay is observed with WLH protocol as compared to other protocols. This concludes that WLH protocol with proposed outlier detection mechanism is better in performance as compared to other protocols. A similar trend is observed for 150 nodes as shown in figure 10. Performance of Teo & Tan protocol is observed better as compared to other protocols with 5 pkt/sec. With increase in packet rate, end-to-end delay reduces because more packets are available for route establishment and data transfer.

V. CONCLUSION

Multi-layered outlier detection process through

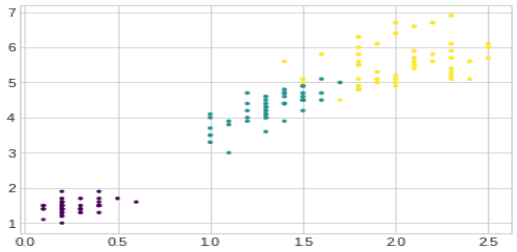


Figure 2: Initial nodes distribution (time = 100 sec.)

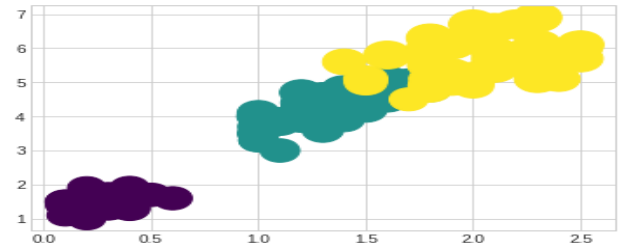


Figure 3: Initial cluster formation (time = 100 sec.)

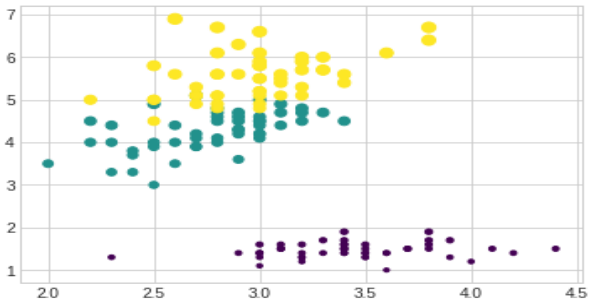


Figure 4: Initial nodes distribution (time = 200 sec.)

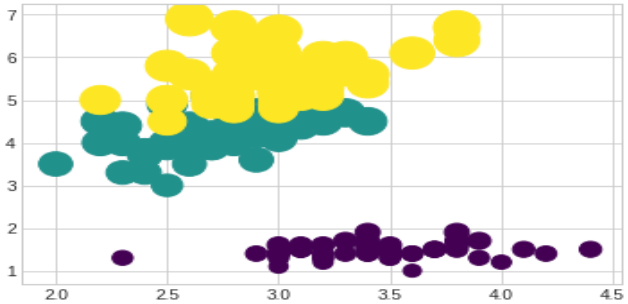


Figure 5: Initial cluster formation (time = 200 sec.)

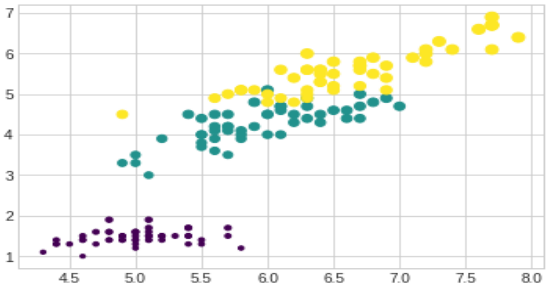


Figure 6: Initial nodes distribution (time = 500 sec.)

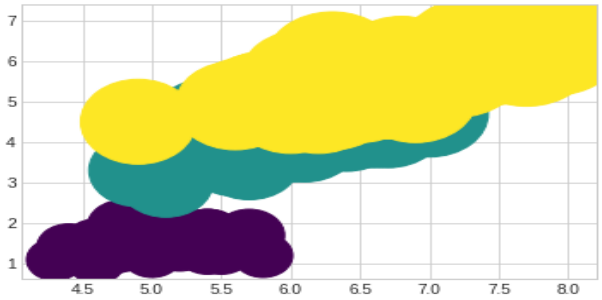
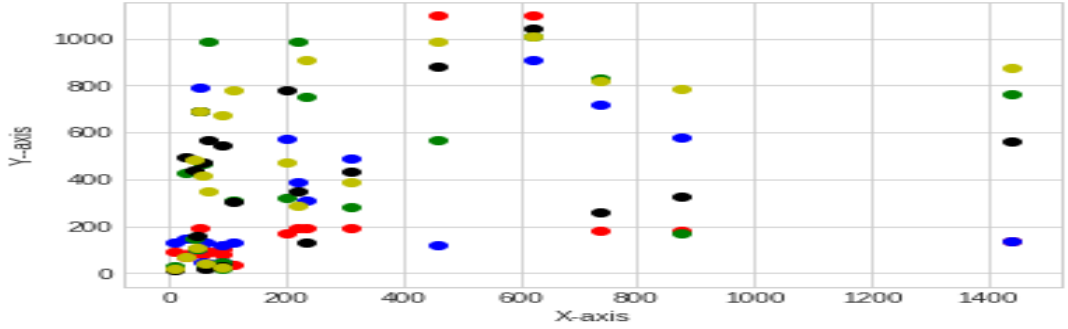


Figure 7: Initial cluster formation (time = 500 sec.)



(Laye-1: Red, Layer-2: Blue, Layer-3: Green, Layer-4: Black, Layer-5: Yellow)

Figure 8: Detection of outliers after each layer processing

anomaly calculation is considered to be efficient approach in terms of performance analysis. This work proposes a similar multi-layered approach for hierarchical key management process. In this hierarchical key management, keys are generated and distributed using different lightweight key mechanisms. These mechanisms used cryptography primitives and protocols for providing security. This performance based outlier detection mechanism analysis the lightweight key management protocols from functionalities of different protocol stack layers. In simulation, results are analyzed for 75 and 150 nodes networks. Results shows that WLH protocol is considered to be the lightest protocol in terms of throughput and end-to-end delay as compared to Teo & Tan, and Tseng's protocols. Although throughput is least for Teo & Tan protocol initially but it shows maximum improvement and maximum value as compared to other protocols. In terms of end-to-end delay, Teo & Tan protocol shows minimum delay with maximum packet rate. Thus, Teo & Tan protocol is consider to be better as compared to other protocols. Visualization process presents each layer's outcome and cluster formation, and an outlier detection process performs a comparative analysis of each layer's outcome with final outlier detected nodes.

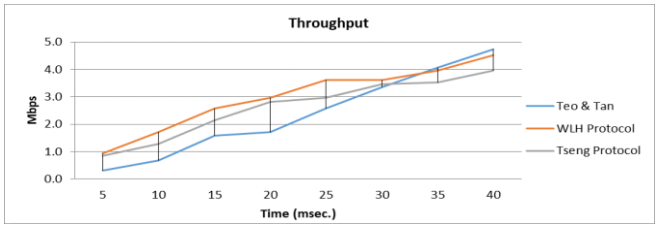


Figure 9: Comparative analysis of throughput for lightweight key management protocols.

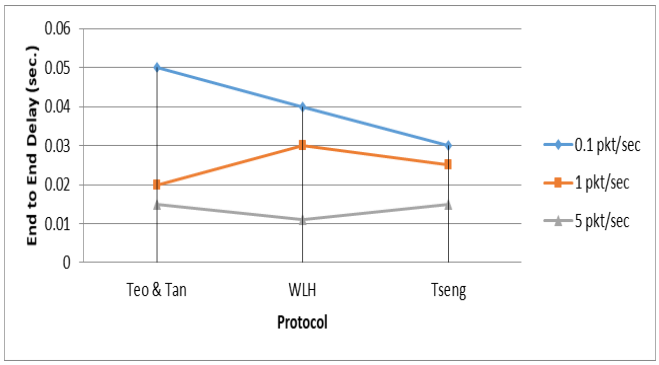


Figure 10: Comparative analysis of End-to-End Delay for 75 nodes network.

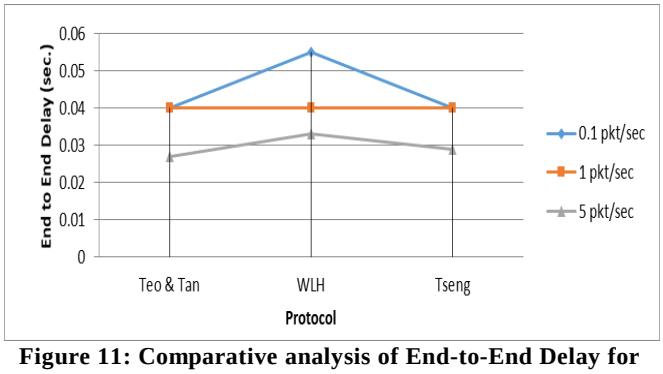


Figure 11: Comparative analysis of End-to-End Delay for 150 nodes network

ACKNOWLEDGMENT

This work is part of a research project sponsored from UPES SEED Division (Project Grant ID: UPES/R&D/180918/14, Project Website: https://sites.google.com/view/adarshproject2/)

REFERENCES

1. A. Kumar, A. Aggarwal, Charu, "Efficient hierarchical threshold symmetric group key management protocol for mobile ad hoc networks," *Proc. Int. Conf. on Contemporary Computing (IC3)*, Noida, India, pp. 335-346, August 2012.
2. J. C. M. Teo and C. H. Tan, "Energy-Efficient and Scalable Group Key Agreement for Large Ad Hoc Networks," PE-WASUN's 05, pp. 114-121, October 10-13, 2005.
3. H. A. Wen, C. L. Lin and T. Hwang, "Provably secure authenticated key exchange protocols for low power computing clients", *Computers and Security*, vol. 25, pp. 106-113, 2006.
4. Brita Vesteras, "Analysis of Key Agreement Protocols," Master's Thesis Report, Department of Computer Science and Media Technology, Gjovik University College, 2006.
5. Y. M. Tseng, "Efficient authenticated key agreement protocols resistant to a denial of service attack," *International Journal of Network Management*, vol. 15, pp. 193-202, 2005.
6. Y. M. Tseng, "Cryptanalysis and improvement of key distribution system for csat satellite communication," *Informatica*, vol. 13, no. 3, pp. 369-376, 2002.
7. Y. M. Tseng, "An improved conference key agreement protocol with forward secrecy," *Informatica*, vol. 16, no. 2, pp. 275-284, 2005.
8. I. Krontiris, T. Giannetsos and T. Dimitriou, "LIDeA: a distributed lightweight intrusion detection architecture for sensor networks," *Proc. 4th Inter. Conf. on Security and Privacy in Communication Networks*, p. 20, Sep. 2008.
9. A. F. Farhan, D. Zulkhairi and M. T. Hatim, "Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach," *Proc. 4th IEEE/IFIP Inter. Conf. on Internet (ICI-2008)*, pp. 1-5, 2008,
10. S. Kumar and K. Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges," *Security and Communication Networks*, vol. 9, no. 14, pp. 2484-2556, 2016..
11. M. A. Zamil and S. Samarah, "Applications of Data Mining Techniques for Vehicular Ad hoc Networks", *arXiv preprint arXiv:1807.02564*, 2018.
12. M. Uddin, A. A. Rahman, N. Uddin, J. Memon, R. A. Alsaqour and D. Kazi, "Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents," *IJ Network Security*, vol. 15, no. 2, pp.97-105, 2013.

AUTHORS PROFILE

Mr Saurabh Jain received his Master Degree(M.Tech) in Information Security from MANIT,Bhopal Madhya Pradesh,India in 2012,and persuing his PhD in Computer Science & Engineering from University of Petroleum and Energy Studies Dehradun, India, He has worked as an Assistant Professor in Computer Science and Engineering Department at Oriental College of Technology, Bhopal. In the past he has acted as a Head of Department in Computer Science and Engineering Department at Oriental College of Technology, Bhopal. Several other responsibilities that he has undertaken include Remote Center Coordinator of Oriental College of Technology (RC ID: 1123), a Lecturer at department of Information Technology in Bansal Institute of Science & Technology, Bhopal, and currently working as an Assistant Professor in School of Computer Science and (SoCS) at University of Petroleum & Energy Studies, Dehradun. Mr Saurabh has published 15+ research papers in reputed journals and conferences and conducted various International and national conferences, conducted multiple workshops under the mission for training of T10KT through NMEICT IIT Bombay funded by MHRD, Govt. of India. He is a certified QCSP (Quick Heal Academy Certified Cyber Security Professional) in 2018 and his research interest lies in Information, Network and web Security.

Neeraj Chugh is an Assistant Professor in University of Petroleum & Energy Studies, Dehradun, India and enrolled in PhD (CSE) from Uttrakhand Technical University (UTU), Uttrakhand, India. He received his M. Tech. (CSE) from Kurukshetra University Kurukshetra, India in 2001. His research interests includes Database Management system, Data Mining, and Outlier/Anomaly detection and event detection in sensor networks.

Dr. Adarsh Kumar received his Master degree (M. Tech) in Software Engineering from Thapar University, Patiala, Punjab, India, in 2005 and earned his PhD degree from Jaypee Institute of Information Technology University, Noida, India in 2016 followed by Post-Doc from Software Research Institute, Athlone Institute of Technology, Ireleand during 2016-2018. From 2005 to 2016, he has been associated with the Department of Computer Science Engineering & Information Technology, Jaypee Institute of Information Technology, Noida, Uttar-Pardesh, India, where he worked as Assistant Professor. Currently, he is working with University of Petroleum & Energy Studies, Dehradun, India as Associate Professor in School of Computer Science. His main research interests are cybersecurity, cryptography, network security, and ad-hoc networks. He has published 35+ research papers in reputed journals, conferences and workshops. He participated in one European Union H2020 sponsored research project and he is currently executing two research projects sponsored from UPES SEED division.

Dr. Alok Aggarwal his bachelors' and masters' degrees in Computer Science & Engineering in 1995 and 2001 respectively and his PhD degree in Engineering from IIT Roorkee, Roorkee, India in 2010. He has academic experience of 18 years, industry experience of 4 years and research experience of 5 years. He has contributed more than 175 research contributions in different journals and conference proceedings. Currently he is working with University of Petroleum & Energy Studies, Dehradun, India as Professor in CSE department.

Dr. Neelu Jyoti Ahuja Dr. Neelu Jyothi Ahuja is a Professor and Head-Department of Systemics, at School of Computer Science at University of Petroleum and Energy Studies, Dehradun. Her PhD awarded in 2010, was on development of a prototype rule based expert system for seismic data interpretation. Apart from academic teaching at university level, she is an active researcher. From period of 2010 to 2017, she has been head of Research Centre-Computing Research Institute, spearheading intra-disciplinary research and coordinating research activities. She holds 20+ years of experience in teaching, research and project proposal development and has published papers in journals and conferences at international and national level.