Non-Interactive Zero Knowledge Proofs for the Authentication of IoT Devices in Reduced Connectivity Environments

Marcus Walshe[a], Gregory Epiphaniou[b,*], Haider Al-Khateeb[b], Mohammad Hammoudeh[c], Vasilios Katos[d], Ali Dehghantanha[e]

[a]*Department of Computer Science and Digital Technologies, University of Northumbria, Newcastle, E1 7HT, UK*
[b]*Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, WV1 1LY, UK*
[c]*Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, M15 6BH, UK*
[d]*Department of Computer Science, Bournemouth University, UK, BH12 5BB*
[e]*Security of Advanced Systems Lab, School of Computer Science, University of Guelph, Ontario, Canada*

Abstract

Current authentication protocols seek to establish authenticated sessions over insecure channels while maintaining a small footprint considering the energy consumption and computational overheads. Traditional authentication schemes must store a form of authentication data on the devices, putting this data at risk. Approaches based on purely public/private key infrastructure come with additional computation and maintenance costs. This work proposes a novel non-interactive zero-knowledge (NIZKP) authentication protocol that incorporates the limiting factors in IoT communication devices and sensors. Our protocol considers the inherent network instability and replaces the ZKP NP-hard problem using the Merkle tree structure for the creation of the authentication challenge. A series of simulations evaluate the performance of NIZKP against traditional ZKP approaches based on graph isomorphism. A set of performance metrics has been used, namely the channel rounds for client authentication, ef-

*g.epiphaniou@wlv.ac.uk
Email addresses: `walshe.msc@gmail.com` (Marcus Walshe), `g.epiphaniou@wlv.ac.uk` (Gregory Epiphaniou), `h.al-khateeb@wlv.ac.uk` (Haider Al-Khateeb), `M.Hammoudeh@mmu.ac.uk` (Mohammad Hammoudeh), `vkatos@bournemouth.ac.uk` (Vasilios Katos), `adehghan@uoguelph.ca` (Ali Dehghantanha)

fects of the authentication processes, and the protocol interactions to determine areas of improvements. The simulation results indicate empirical evidence for the suitability of our NIKP approach for authentication purposes in resource-constrained IoT environments.

Keywords: IoT, ZKP, NIZKP, Authentication, WSN, ANOVA.

---

1. Introduction

The Internet of Things (IoT) paradigm has become the driving factor for the exponential increase of inter-connected devices and sensors. These devices have gradually evolved from sensing the environment to data processing and decision-making. These enabled better user experience, but also, an alarmingly increased attack surface against traditional confidentiality, integrity and availability aspects [1]. The "things" are connected via wireless links to form complex and often pervasive Wireless Sensor Networks (WSN) with suitable resources and interfaces to information that can be relayed back to source nodes.

There is a variety of applications for IoT ranging from wearable computing, healthcare to supply chain monitoring and military [2],[3],[4],[5], [6], [7]. The necessity to authenticate entities (participants) and attribute associated actions in WSN is of paramount importance [8]. The communication in these networks often includes unauthenticated participants allowing threat actors to abuse network components in a variety of ways. This abuse is often manifested as targetted and multi-stage cyber attacks, passive or active eavesdropping, Denial of Service (DoS) and the insertion of rogue sensors affecting the integrity and availability of data [9]. The increase in intra-sensor communication in WSN opens a new area of attacks, since a participant can aggregate modified messages from different participants within the network. Given that malicious nodes can access network resources arbitrarily, the security of these aggregation processes that often include data processing is also essential for the efficacy and feasibility of these networks [10].

Due to the broadcast nature of WSN, different vector of attacks can be man-

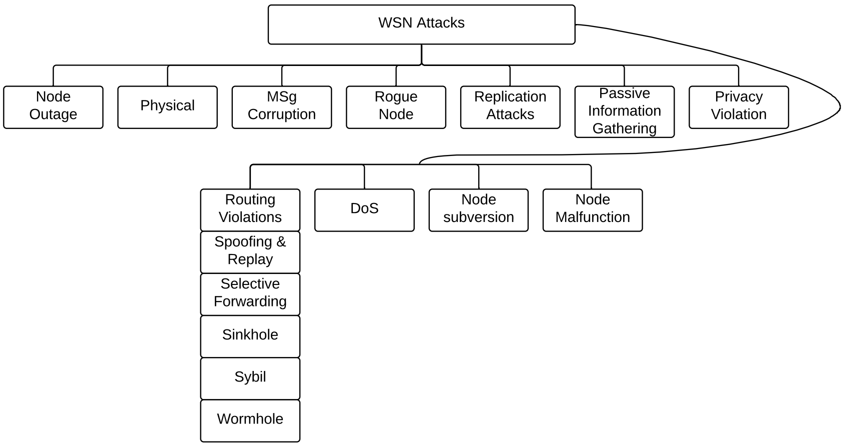

Figure 1: Attacks in WSN [11].

ifested at the network layer. A malicious node can selectively drop packets and actively or passively inspect traffic. The assumption is that often these nodes are considered trustworthy when they forward messages within the network [11], [12]. Compromised nodes can be used as sinkholes to concentrate network traffic and perform traffic analysis to identify communication patterns. In Sybil attacks, a malicious node can co-exist in multiple locations in an attempt to compromise fault-tolerant schemes affecting both data integrity and availability to legitimate resources [13]. In addition, malicious nodes can also record and re-play packets in different locations within the target network. This type of attack known as wormhole, is particularly dangerous as it gives a false perception of proximity to legitimate nodes. It also prevents routing packets from being discovered [14]. Fig. 1 illustrates the main WSN attack categories in terms of their impact.

Strict requirements prior IoT deployment such as aggregation processes and secure integration of services within the network should be considered [15]. In addition, the limited IoT object resources, namely, computation and processing must also be considered when designing authentication protocols for IoT systems. Standards such as IEEE 802.14.4-2015 have been created for the physical and MAC layers to tackle some of these problems [16]. When examining the requirements for authentication protocols, the assumption is that semantic security is offered in WSN and the communication architecture within which the protocols will operate is well established.

The communication architecture is often described by criteria such as the key generation process, the number of participants using the protocol and the mechanisms used to derive session keys. However, where collaborative functions such as data aggregation and node referrals require processing, this can directly contradict the security objectives even if the security requirements have been made explicit as part of the protocols' specifications. When proposing security schemes for WSN, the challenge of maintaining the functionality and network efficiency dictates careful security design and implementation. This challenge increases in locations where network reliability is intermittent and where nodes are in locations where they could be physically compromised [17].

The development of a computationally sound NIZKP challenge value would allow the mitigation of certain threats against authentication assuming that each challenge value is encrypted. The Verifier V must both be able to decrypt the challenge, proving that there is a shared secret key between the Prover P and V preventing impersonation attacks. Extending the security of the challenge packet, the P could include their Universally Unique Identifier (UUID) in the final packet encrypted with the server UUID provided in the initial client server exchange. In addition to confidentiality, should the server decrypt the final packet value, and this does not match the expected server UUID, the authentication challenge can be rejected. Using this extended functionality, from a NIZKP server a log can be generated to store three values, the client UUID, the server UUID and the public challenge for a session. A query of this log every time a client requests authentication would check if the client UUID, server UUID or the public challenge had been used previously, either together or individually. This simple log would provide a multitude of information that could be used in security operation monitoring, performance monitoring and auditing efforts [18]. An auditing function would be vital to monitoring and reporting on login frequency and malicious login attempts in otherwise unsupervised environments.

The remainder of the paper is structured as follows: In Section 2 we discuss existing works in the field of ZKP with emphasis upon authentication design principles of existing protocols. Section 3 focuses on the design and testing of our NIZKP protocol with a detailed explanation of the authentication modules constituting the building blocks using a non-interactive approach. Section 4 presents the results and discussion from our experiments and the evaluation of NIZKP using formal statistical methods against the data produced by our simulations and existing ZKP approaches. In Section 5 we present the threat model for our NIZKP protocol with a description of both threat vectors and mitigations. Finally, Section 6 concludes this work and gives future avenues.

2. Related Works

In IoT systems the requirement for strong security procedures, especially application layer security, has led to the development of multiple authentication protocols, usually modelled on traditional authentication approaches. These schemes are often based on login credentials with stored authentication values or private/public key schemes. Attacks can originate from traditionally expected adversaries located inside or outside the network or from previously trusted nodes acting maliciously [19],[20],[21]. Recent advancements in wearable wireless sensors with quality requirements namely, energy, memory, and computational efficiency further incorporate ZKP to provide lightweight authentication with appropriate commitment schemes [22], [23]. ZKP has also been used as a mean to implement web security models for information exchange over insecure channels.

The authors of [24] have introduced a robust authentication scheme over a secure communication channel in which the registration and login processes for entities is demonstrated. Registered entities can submit their queries to the network within a specific timeframe utterly independent of the application time and only while they move within a designated zone within this time. Should any of these requirements fail, the participant must re-register to the network through this scheme. The scheme is proved to be susceptible to impersonation, stolen V credentials and gateway bypass attacks. An enhanced version of this scheme was introduced in [25] that eliminates some of the attack vectors. This process has been achieved through changes in the authentication steps to include separate phases during login and registration and the addition of a password change capability. However, the enhanced version of the scheme was also found vulnerable to password guessing and impersonation attacks.

The authors in [26] introduced a mutual authentication scheme with session key agreement between a user and an object. Traditional password authentication has been used for the gateway access with a secret generated and stored on different devices within the system. These devices become designated to serve requests from the user. A smart card was also introduced during the login process to enable the device to calculate whether the request has been done within an acceptable timeframe for the session key to be created. Most of the techniques mentioned above rely on user-supplied information at the stage of transfering credentials that are stored to devices within the network. These limitations in existing authentication mechanisms can be partially addressed by the use of Zero-Knowledge proofs (ZKP). ZKPs are considered the cornerstone of modern cryptography on the premise that a proof can be both convincing and yet revealing no information other than the validity of the claim made. The conversation between the P and V must convince the latter about the Prove's claim without the P revealing the details that construct the evidence. The exchange of information must assure beyond any reasonable doubt the validity of $P's$ claim to V. Often this process is repetitive until the legitimacy of $P's$ is fully established. In each step, a reducing probability of $\frac{1}{2}^n$ enables P to guess a response to the challenge presented by V. An inappropriate response to the challenge breaks the authentication process. There is no prior knowledge of the secret, nor changes are possible to publicly shared values without re-executing the commitment protocol. A variation of the ZKP is the Non-Interactive Zero knowledge Proof (NIZKP), in which there is no continuous interaction between V and the P as in the manner of the ZKP. The P still wishes to assure beyond doubt their claim of validity to the V, however, rather than reply in multiple interactive challenge rounds between the P and V, the ZKP proofs are computed and then distributed by the P to the V. The V can then validate multiple claims without the need to reissue challenges thus reducing computation and communication overhead. In the case of bounded NIZKP the following applies: Given that a random string σ and a single sufficient theorem T, the algorithm outputs in a non-interactive manner a second string in zero-knowledge that T is true for any V who has access to the same string σ. The authors of [27] define the bounded NIZKP scheme as follows:

Completeness: For all $x \in L_n$ and for sufficient large n,

$$Pr(\sigma \overset{\text{R}}{\leftarrow} \{0,1\}^{n^c}; Proof \overset{\text{R}}{\leftarrow} Prover(\sigma, x) : Verifier(\sigma, x, Proof) = 1 > 2/3 \tag{1}$$

soundness: For all $x \in L_n$ for all turing machines Prover', and for all sufficiently large n,

$$Pr(\sigma \overset{\text{R}}{\leftarrow} \{0,1\}^{n^c}; Proof \overset{\text{R}}{\leftarrow} Prover'(\sigma, x) : Verifier(\sigma, x, Proof) = 1 < 2/3 \tag{2}$$

Zero-knowledge: An algorithm S such as $x \in L_n$ for all non-uniform algorithms D, for all $d > 0$, and all sufficiently large n,

$$|Pr(s \overset{\text{R}}{\leftarrow} View(n, x) : D_n(s) = 1) - Pr(s \overset{\text{R}}{\leftarrow} S(1^n, x) : Dn(s) - 1)| < n^{-d}, \tag{3}$$

where,

$$View(n, x) = \left\{\sigma \overset{\text{R}}{\leftarrow} \{0,1\}^{n^c}; Proof \overset{\text{R}}{\leftarrow} Prover(\sigma, x) : (x, \sigma, Proof)\right\} \tag{4}$$

The authors of [28] have adopted ZKP for identity verification with emphasis on completeness where valid inputs can be proved on any protocol run and soundness where no malicious P or V can derive the secret from the interactions.

Several authentication schemes seem to have incorporated ZKPs particularly within the context of Privacy Enhancement Technologies (PET), electronic voting schemes, anonymous blacklisting systems, and prevention of Denial of Service (DoS) attacks [29], [30],[31],[32]. Common across all approaches is the obligation of each participant to prove certain honesty in the execution of authentication processes. The ZKP in all cases plays a critical role in concealing the sensitive information within the network. The number of the required subsequent rounds of proof required and the associate cost of resources remains an issue in the construction of each ZKP. However, ZKP can be a perfect authentication candidate in cases that use of password-based approaches and PKI are either computationally expensive or impractical. Typical scenarios include authentication for the IoT with low or intermitted connectivity and strict energy preservation requirements related to the computational complexity of security operations.

The authors in [33] use a graph isomorphism-based scheme with a well defined ZKP problem where graphs are expected to grow in order to satisfy the security requirements. The authors introduced a variant of NIZKP using a single message to verify the knowledge. They also introduced the notion of different levels of security as a function of the number of challenges exchanged increasing the level of safety for the V. The use of the cryptographic cutting function has been used as a key requirement within the scheme to fulfil the computational assumptions about the cryptographic checksum needed. This scheme uses broadcast messages to identify legitimate network nodes and the commitment is decrypted only if decryption of the previous submitted messages is successful. The results were emphasised in the polynomial tendancy between the size of the segments and the number of nodes of the graph that represents the network. The authors have also investigated the segment generation time with different devices as a function of the serialisation of graphs. As expected they reported high computational time to build the package although some cost was attributed to the programming language used for the implementation.

Merkle trees and predetermined timestamps have been used in a scheme introduced by [34]. Many cryptographic schemes deploy Merkle trees that establish specific relationships between a tree leaf value and the root node value so as the authenticity of the latter can be established. Sibling leaves are combined and hashed to form a parent leaf repetitively. The traversal mechanism developed allows the values from all leaves to be stored outside the memory space which is regarded as a resource intensive and inefficient process [35].

The problem of information leakage has been researched in peer-to-peer (P2P) authentication systems as a key component of the security resistance of identity-based approaches. The authors of [36] introduced a pseudo-trust scheme where ZKP is used for authentication using anonymous communications. The resistance of the scheme was tested against certain man-in-the-middle (MITM) attacks using universal hashing and ZKP as an approach to bind pseudo-identities to the authentication paths. A similar approach has been presented in [37] to address phishing and eavesdropping in single-sign-on services (SSO) and transmission of user profiles across multiple platforms such as mobile phones and web applications. The potential to increase privacy and security using ZKP has been recently exploited in blockchain applications using a modified version of Di Crescenzo and Lipmaa's protocol in [38]. The work reduces the size of both the proofs and the computational complexity required for the verification process. Initial data can also be obtained by device fingerprinting and geo-fencing techniques that allow the verification to be completed prior to the creation of the authentication challenge [39].

A common concern amongst the reviewed literature is the adaptation of ZKP protocols for the transmission of assets across a distributed P2P blockchain network. This area seems to attract much of the research efforts with focus on the privacy preservation aspects of the communication [**?**],[40]. The transaction verification is the only piece of information needed without exposing information about the sender, the recipient or assets.

The demand for lightweight authentication schemes in the IoT domain and their importance has driven certain developments in the use of ZKP as a viable solution [41], [42], [43]. Finally, the authors in [44] define a web security model consists of multiple layers such as the interface, application, and database to execute control functionalities and optimise authentication and application versatility.

3. NIZKP Design

Our NIZKP protocol consists of two main authentication components, namely the client and server module described in Sec. 3.1. During the communication initiation phase, the NIZKP client module sends to NIZKP server module the root node hash to be used as the public commitment for the challenge. The NIZKP client module then proceeds to decimate the Merkle tree, nodes not selected for use in the challenge which are no longer required are destroyed. The NIZKP client module examines the configuration for the minimum number of challenges required to build the challenge packet (defined by configuration). The NIZKP client module then selects the initial candidate nodes for the challenge packet, starting at the appropriate level in the Merkle Tree [1]. For each candidate selected, a secondary binary selection will determine if the candidate or both candidate's child nodes will be selected for the packet. This recursive process will ensure that the NIZKP client module will always produce a challenge packet with the minimum required number of challenges but may also contain a random number of challenges between the minimum challenge value and the maximum node size for the tree. (e.g., Desired challenges = 32, Max Tree Nodes = 512, Challenge Packet Size = min32 $\rightarrow$ max512).

Given the IoT object's limited computational resources and potential for limited network connectivity, this research proposes an authentication protocol based on NIZKP. Where such proofs are utilised, the requirement to store

[1] e.g., desired challenges = 32, Initial tree level = $32log_2$

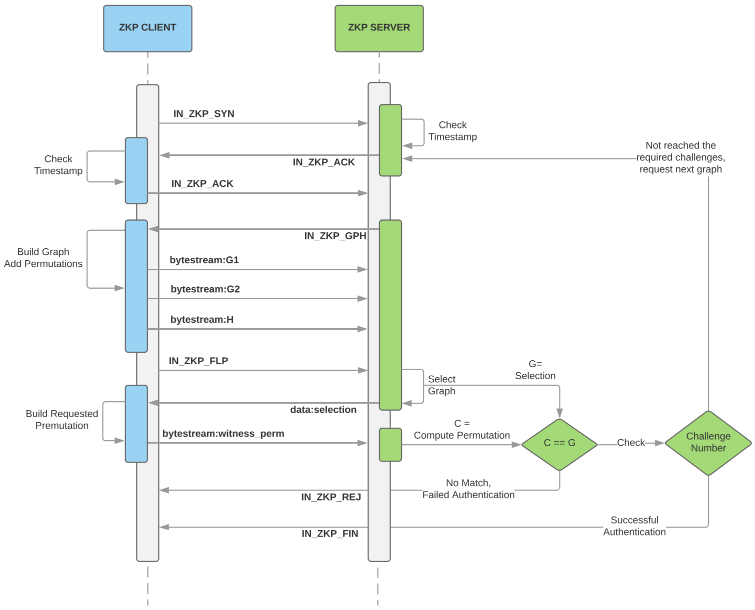

Figure 2: ZKP Client Server Simulation Flow.

authentication information, such as password hashes, is removed therefore to reduce the exposure to attack. NIZKP produces a commitment set of data and provides increased levels of flexibility for authentication in environments without Internet connectivity that often prevents the use of existing schemes based on certification authorities.

The client authentication module produces graphs $G1$ and $G2$ (See Fig. 2). Graph $G1$ is generated automatically and $G2$ is an isomorphism of $G1$. The permutation produced by $G2$ constitutes our secret to be shared between the ZKP server and the V. A third party graph H will be generated as an isomorphism of $G1$. $G1$, $G2$, H are shared between the client and ZKP server modules. The P between all graphs claims a shared isomorphism. Graphs from $G1$, $G2$ are randomly selected by the server and returned to the authentication client to enable isomorphism between each graph and H. When isomorphism is returned by the client in case that $G1$ is selected the return is structured as $\pi^{-1} : H \rightarrow G1$.

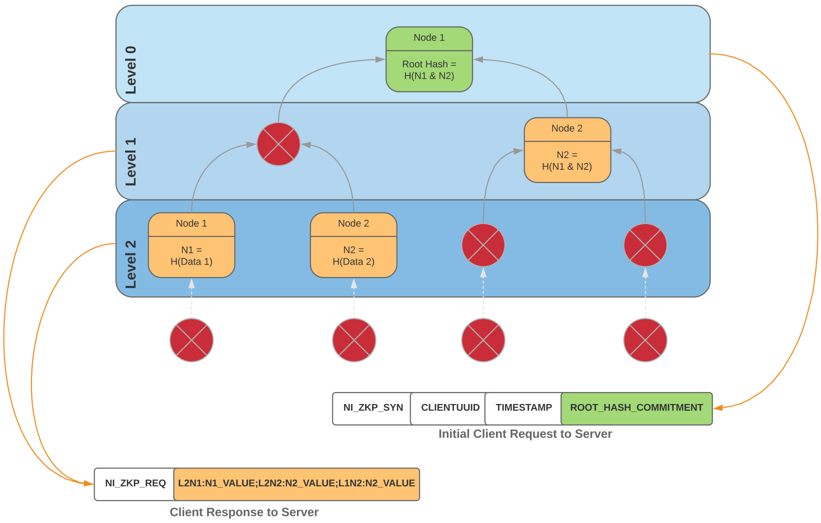

Figure 3: Challenge Packets and Construction of Proof.

The server's permutation is used to confirm that H is indeed isomorphic to the V's chosen graph(s) and accepts the P's (P) claim. The probability of a single graph isomorphic to H is 50% for P including guessing the graph chosen by V. The V can increase confidence with a challenge repeated until $P's$ legitimacy is established. Each repeated challenge reduces the probability of guessing the outcome as $\frac{1}{2}^n$ (chosen graph) thus, increasing the legitimacy of the commitment to V. The authentication attempt is invalidated in cases that P fails to provide an appropriate solution. Once the commitment cycle is completed, both V is unaware of the secret, and P can not alter the publicly shared value for that run of the commitment protocol.

The development and testing of our NIZKP adheres to certain assumptions around its design. The nonces used are not predictable thus replay attacks based on responses are not feasible. The trust relationships in the protocol design have been explicitly defined with every message exchanges' in the challenge packets (See Fig. 3). During our protocol execution, it is easy to deduce to which run each message belongs into with clear conditions defined. The internal mechanics of the algorithm provide the conditions for messages to be acted upon. Although in this work the protocol does not dictate the encryption scheme to be used, the provision for it existing as part of our future work. The assumption is that our protocol supports widely acceptable standards such as iterative block ciphers for the formation and transmission of the encrypted challenge.

3.1. NIZKP Authentication Modules

The NIZKP client module P, generates a 256bit random number as the base data values for a Merkle tree to be build (See Fig. 3). SHA-256 is used for the leaf node creation LN_X creation which includes the checksum value of the lowest level of the Merkle tree with the total count calculated by $node_count = (LN * 2) - 1$ Under the operation of the NIZKP client module, a pair of sibling nodes are concatenated, and their resulting value is hashed. This value is the parent node value $PN = H(SN_n + SN_{n+1})$ with the two contributing nodes being its children. The process only stops when a final single value is calculated, namely the root node hash. The whole packet processing capability and simulation flow for our protocol are illustrated in Fig. 4, 5.

The first communication step involves the root node hash value as public information for the creation of the challenge. The nodes that no longer needed in the challenge process are automatically discarded. The challenge packet is constructed using a minimum number of challenges and examined by the client using a configuration template. The client authentication module selects the candidates for the challenge packet from an appropriate level in the Merkle tree. We define this tree level to $32log_2$ with 32 required challenges. A separate algorithmic process decides on the selection of the candidates' child nodes as part of the construction of the challenge packet. This step is to assure that the selection is always limited to input with enough entropy given the maximum node size of the tree.

During the verification process, a solution to the commitment is requested by V and P supplies the values for the challenge packet previously computed from the Merkle tree in a specially crafted packet. The NIZKP commitment process is

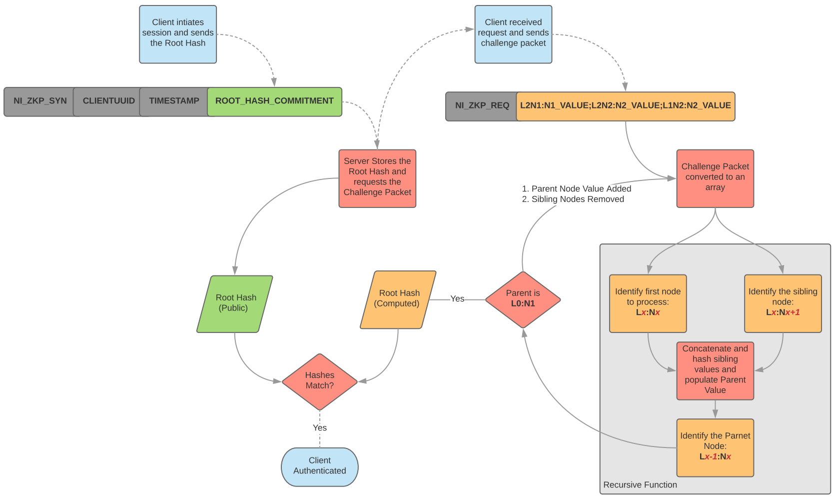

Figure 4: NIZKP Packet Processing.

split into two phases including the actual commitment and verification involving both P and V sharing a universal root hash as calculated and shared by P. A selection of modes from the Merkle tree is sent from P to V for processing as part of the verification process. Successful verification of the root node hash by V renders the authentication attempt as successful.

3.2. Simulation Setup and Datasets

A series of simulations have been run following the principles in [45] to construct the essential client/server communications with all elements coded in Python using common design patterns. Traffic handling is achieved through Python sockets and the authentication modules of NIZKP have been implemented using dedicated message blocks. These simulations have been used to collect primary data for each device utilising our protocol. Our simulations utilise a single threaded socket client/server for auditing and logging. Each authentication algorithm will be tested using the same device code for consistency across our experiments using common test harness during simulations. The appropriate authentication module code was looped to fulfil the required number

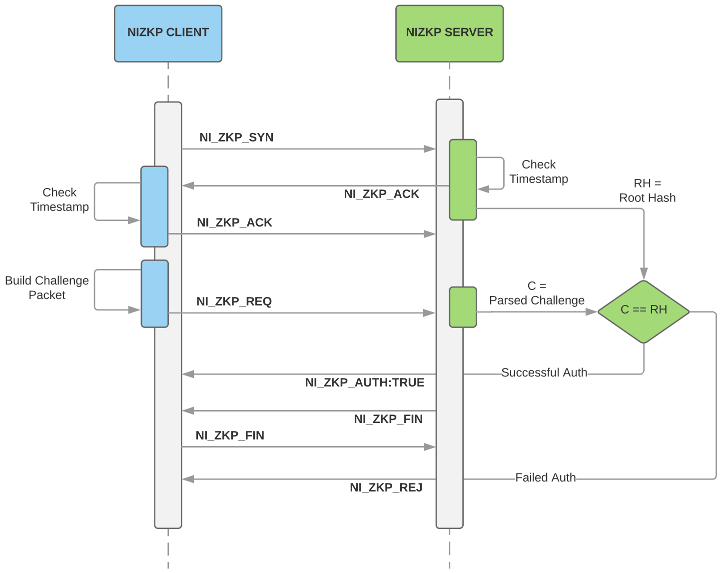

Figure 5: NIZKP Client Server Message Exchange.

of iterations during testing.

The datasets created as part of our simulations consist of a combination of both ZKP and NIZKP with sample sizes of $N = 10,000$. We estimated 5,000 iterations for each pair to provide 10,000 results. The tests were repeated for challenge requests of 16, 32, 64, 128 and 256 against each proof creating a final dataset of $N = 50,000$ for each replicated test. We employ a positivist philosophy to eliminate self-developed constructs and measure only observable, repetitive and comparative dataset leading to re-producible scientific outputs. We also constructed a clear set of hypotheses for testing, which is described in Section 4.

4. Results and discussion

The data collected during our experiments is used for the evaluation of the client authentication module. Client authentication will be tested against each algorithm using an increasing number of proof challenges, analogous to increasing confidence in the authentication. A Two way Analysis of Variance (ANOVA) with replication is used to test the data and formulate three null hypotheses to be examined as follows:

Hypothesis 1 (H1): *H0: The number of challenges do not have any significant effect on the response. Ha: Rejection of the First Null Hypothesis means the number of challenges is significant.*

Hypothesis 2 (H2): *H0: The authentication proof algorithm does not have a significant effect on the response. Ha: Rejection of the Second Null Hypothesis means the authentication proof algorithm factor is significant.*

Hypothesis 3 (H3): *H0: The interaction between the challenges and authentication proof does not pose a significant effect on the response. Ha: Rejection of the Third Null Hypothesis means that an effect from the interaction of challenges and authentication proof algorithm factors is significant.*

The choice of the client authentication time, from initiation of authentication request to receipt of successful authentication, has been selected to test the proposed theory. Using a NIZKP, will preclude other measurement metrics, e.g., NIZKP will always use less network traffic by design so this must be excluded, less traffic and associated overhead means measurement of traffic size must also be excluded. The outcome measurement will consider time as a dependant variable. This will not be a consideration for the determination of the result alone as multiple factors can influence running time and so is usually considered a poor metric to observe, but rather as a ratio difference of performance between the two algorithms. Should the design of the experiment or simulations used to gather data be flawed, any analysis results based on that data set is of questionable quality. Data gathered during the simulations are used for statistical study using an Analysis of Variance (ANOVA) statistical model. Any informed decisions based on this study are only as sound as the methods used to obtain the data. A longitudinal time horizon involving repeated observations of the same variables has been employed to provide large numbers of repeated samples from which to perform analysis and inform conclusions. The datasets are tested prior to the final analyses to ensure that the data gathered from the simulation is appropriate for factorial testing.

The simulation experiments used in this study produced data sets derived by repeated measurement on the same set of subjects under differing conditions. Pairing occurs where subject groups are linked and values are related. The proof challenge number were deliberately paired to match baseline characteristics providing appropriate data for two-way ANOVA testing. A confidence level of %95 has been used throughout our testing with any observed value during our p-value analysis below 0.005 rejecting our hypotheses. Alternatively, the null hypothesis is accepted given the observed factor has no effect on the result. The data has been tested against Bartlett's Test of Sphericity to compare the correlation matrix to the identity matrix to avoid redundancy between variables. A failure in the test should indicate a correlation matrix identical to an identity matrix. Since an alternative authentication protocol is proposed we only observe the results of the BTS with $p \leq .050$. The testing hypothesis $H0$: state the variance is identical or Ha : at least one of the variances is different from another. For Bartlett's test, the computed p-value is lower than the significance level ($\alpha = 0.05$), the risk to reject the null hypothesis $H0$ while it is true is lower than 0.01% (See Table 1).

We also measured the sampling accuracy on our simulation data using Kaiser-Mayer-Olking test (KMO). Compact correlation patterns are indicated by results close to 1 rendering the factors distinct and reliable in our factor analysis. The results of the KMO test deemed as just acceptable if the result is > 0.5, average $0.5 \sim 0.7$, good for $0.7 \sim 0.8$, and excellent for > 0.8. For each dataset paired KMO values were separated and results obtained with a range spread to indicate appropriateness. The data gathered was an excellent candidate for factorial testing (See Table 2). A two-way ANOVA allowed the examination of two factors in a single experiment where we facilitate repeated data collection. To ensure accurate and reproducible results we also considered the following

Table 1: Bartlett's Test of Sphericity

Bartlett's Test of Sphericity	
Chi-square (Observed value)	267.485
Chi-square (Critical value)	16.919
DF	9
p-value (Two-tailed)	<0.0001
alpha	0.05

factors: (1) The experiment consists of two participants (client, server) with standard data logging and collection methods. All modified authentication protocols have been included as part of the participants' interaction during our simulations. (2) Each round of authentication is considered as a single test. (3) We performed tests in cycles of 1,000 and replicated five times for each configuration of authentication challenges. We used Measured System Analysis (MSA) to measure the accuracy and precision in data collection. MSA is used as mean to quantify the accuracy, precision and stability of an experimental design in terms of the data produced. This allows us to experimentally determine the amount of variations existed within our measurement process and quantify variability in our results during the hypotheses testing. MSA is effective in our experiments to assure that data collected and analysed is appropriate for increasing the reliability during our testing and determine the likely source of variation in our data.

The analysis on the homogeneity of variance in the group data was based on the hypothesis that (H0) there are differences between variables and (Ha) there are no differences between variables. The test against the collected dataset seeks to explore the significance of variance between the authentication algorithm and the number of challenges performed.

Table 3 illustrates the statistical significance between the authentication algorithm and challenges. Further changes to either the algorithm or the challenges will have a significant impact on the time required to complete a single

Table 2: Kaiser-Meyer-Olking Measure of Sampling Accuracy

KMO	Measure of Samp. Accur.
NI_ZKP_16	0.995
ZKP_16	0.986
NI_ZKP_32	0.994
ZKP_32	0.933
NI_ZKP_64	0.995
ZKP_64	0.943
NI_ZKP_128	0.995
ZKP_128	0.979
NI_ZKP_256	0.994
ZKP_256	0.989
KMO	0.977

Table 3: ANOVA Test 1: Significance of Algorithm and Challenges

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
Algorithm	1	0.8956	0.8956	1155.6	<2e-16 ***
Challenges	4	1.8327	0.4582	591.2	<2e-16 ***
Residuals	1494	1.1579	0.0008		

Table 4: Tukey Multiple Pairwise-Comparison

	Difference	Lower Value	Upper Value	p adj.
x32-x16	0.004218603	0.002409931	0.006027276	0
x64-x16	0.01725294	0.015444267	0.019061613	0
x128-x16	0.043104083	0.041295411	0.044912756	0
x256-x16	0.095028167	0.093219494	0.096836839	0
x64-x32	0.013034337	0.011225664	0.014843009	0
x128-x32	0.03888548	0.037076807	0.040694153	0
x256-x32	0.090809563	0.089000891	0.092618236	0
x128-x64	0.025851143	0.024042471	0.027659816	0
x256-x64	0.077775227	0.075966554	0.079583899	0
x256-x128	0.051924083	0.050115411	0.053732756	0

Table 5: Pairwise T-Test

	X16	X32	X64	X128
X32	0.16	-	-	-
X64	1.8e-08	2.0e-05	-	-
x128	<2e-16	<2e-16	<2e-16	-
X256	<2e-16	<2e-16	<2e-16	<2e-16

protocol run. The significance of the impact has been measured through the examination of the factors' interaction and the results determine whether the null hypotheses $H0$, Ha can be accepted or rejected as a function of the significance level of p (if $p \leq .50$, $H0$ should be rejected and Ha is accepted).

Table 6 also shows a statistical significance between the interaction of the factors algorithm and the challenges where the p-value ($< 2e-16$) of algorithm is significant indicates association between its selection and the authentication challenge's duration. The p-value ($< 2e - 16$) of challenge is significant indicates an associative relationship between the number of challenges required and the duration of the authentication challenge. Finally, the p-value ($< 2e - 16$) for the interaction between the two factors indicates a strong dependence of the duration of authentication challenge and the relationship of algorithm and challenges. Significant p-value results also indicate differences between group means.

This difference can be better understood by a multiple pairwise-comparison test (See Table 4). The adjusted p-values for each of the pairwise-comparison for the authentication challenges reported results of significance ($padj. < 0.5$). Table 5 illustrates the significance in the combinations confirmed by a pairwise t-test following correction for multiple testing. A normal distribution is assumed following the ANOVA tests carried out including the homogeneity of variance (Fig 6). The Residuals vs Fitted plot is used to check for violations in our model assumptions, in particular, any occurrences of heteroscedasticity, non-linear relationships among the response variables and predictors, unequal error variances and detected outliers. The Residuals versus Fitted plot shows no evidence of association between fitted values and residuals (detected outliers but fall within acceptable criteria), therefore homogeny of variances can be assumed. The results from the Bartlett's test are consistent with this observation. The data presents a normal distribution as reported by both ANOVA and Shapiro-Wilk test against ANOVA residuals ($W = 0.89995$, $p - value < 2.2e - 16$). The ANOVA testing assumes variance is equal across samples and that sample data is normally distributed. If unequal group sizes are used during ANOVA testing, homogeneity of variance will be violated. Large sample variances when observed in small sample sizes can lead to underestimating the significance level and falsely rejecting the null hypothesis. Conversely, where large variances are observed in large group sizes, the significance level may be overestimated, decreasing the validity of the tests performed.

Fig. 7 illustrates the normality plot of residuals with data following the reference line which shows that our sample data is valid. Based on this analysis of the collected data, the results and accuracy of the ANOVA testing, the hypotheses can be evaluated against these findings.

Table 6: ANOVA Test 2: Significance of Interaction of Auth. Algorithm and Challenges

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
Algorithm	1	0.8956	0.8956	13614	<2e-16 ***
Challenges	4	1.8327	0.4582	6965	<2e-16 ***
Algorithm:Challenges	4	1.0598	0.2650	4028	<2e-16 ***
Residuals	1490	0.0980	0.0001		

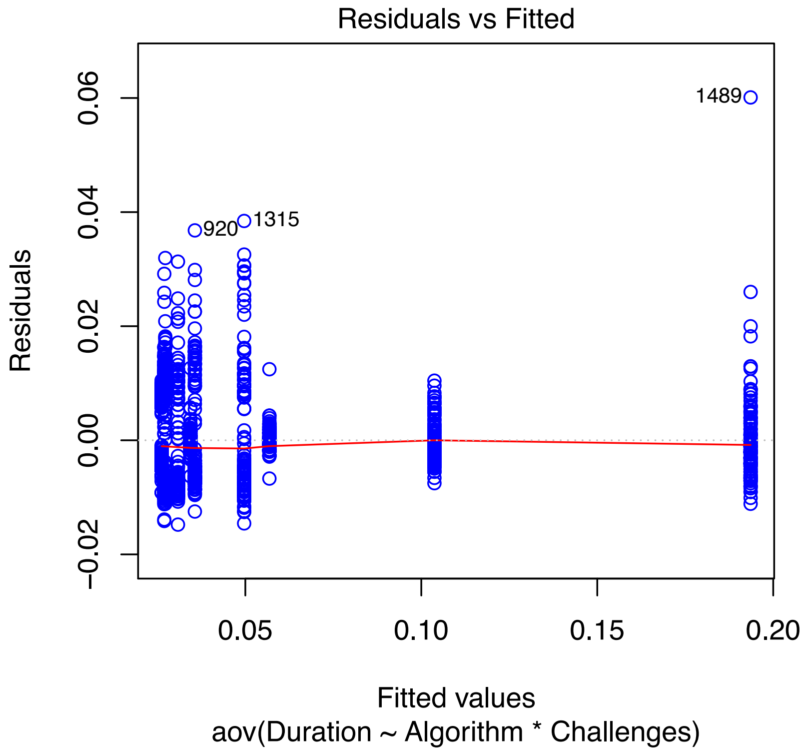

Figure 6: Residuals Vs Fitted Plot.

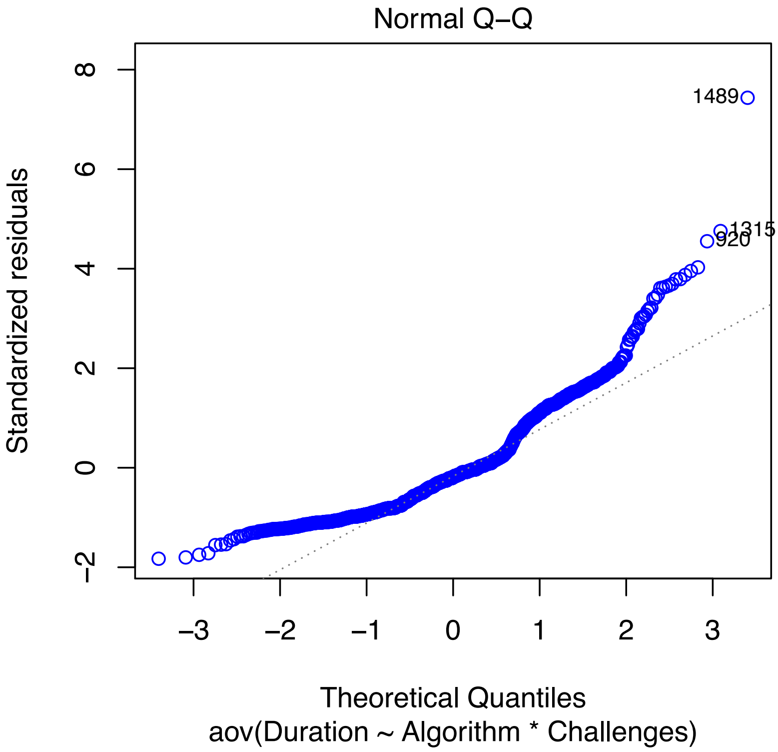

Figure 7: Normal Distribution Plot.

4.1. Hypothesis Testing

We introduced multiple rounds of challenges in our simulations to probe on algorithm's performance and the effect of the increased challenges to the its overall authentication overhead. Given that a V must be of the legitimacy of a P, we repeat the protocol rounds to decrease the probability of guessing the answers to the V's challenges. Hypothesis 1 ($H1$) proves no significant effect on the authentication times on the client device, as a function of the increased challenges used in the authentication protocol. The ANOVA test shown noticeable results for $H1$ as challenges p-value is smaller than ($p \leq .050$)

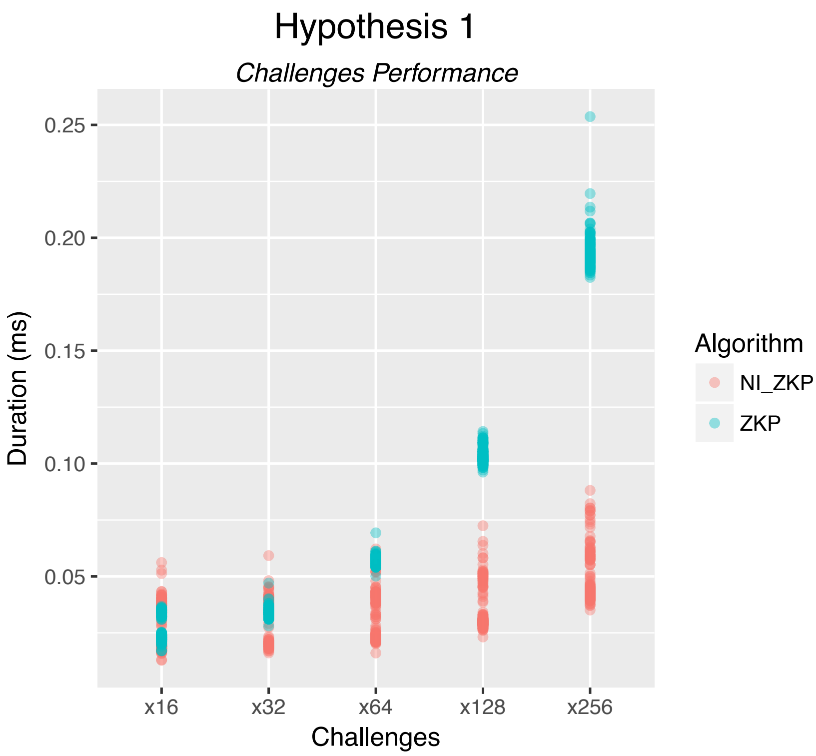

Figure 8: Effect of Authentication Challenges.

rendering the value insignificant (See Fig. 8).

- **Rejected** - *H0: There is no significant effect from the number of challenges factor on the response.*
- **Accepted** - *Ha: Rejection of the First Null Hypothesis, the number of challenges is significant.*

For Hypothesis 2 ($H2$) we focused on the implementation of two different ZKP algorithms with multiple rounds of challenges used as a block to allow the V to build confidence in P's claim. The NIZKP focuses on the same operation

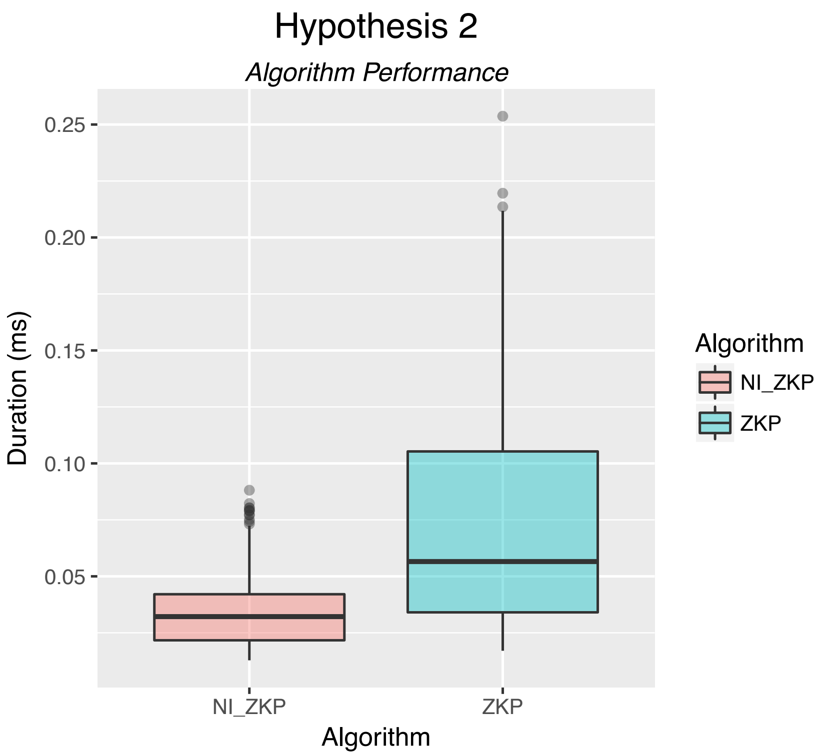

Figure 9: Effect of Authentication Algorithm.

where multiple proofs are created and processed in batches removing the necessity for a repeated communication between the the P and the V. All challenges are sent to the V using a single communication and the V accepts or rejects the proof after processing the message received. Hypothesis 2 $H0$ predicts no significant effect from the authentication proof factor on the response indicating significance of the former. Also, results suggest that p-value is smaller than the significance level ($p \leq .050$) as illustrated in Fig. 9.

- **Rejected** - *H0: No significant effect from the authentication proof algorithm on the response.*

- **Accepted** - *Ha: Rejection of the Second Null Hypothesis, the authentication proof algorithm factor is significant.*

Our simulations used both interactive and non-interactive methods for the authentication process with increased number of challenges. While both methods use ZKP actions to realise their operation, the communication and interaction profiles between them are different. Their effectiveness is demonstrated through the modification of challenges in each round of the authentication process for each method. Hypothesis 3 ($H3$), predicts that there is no significant effect from the interaction of challenges and authentication proof algorithm factors on the response (See Fig. 10. Again, a significant result is returned from the ANOVA test, the Algorithm p-value is again many times smaller than the level of significance ($p \leq .050$).

- **Rejected** - *H0: There is no significant effect from the interaction of challenges and authentication proof algorithm factors on the response.*
- **Accepted** - *Ha: Rejection of the Third Null Hypothesis means that effect from the interaction of challenges and authentication proof algorithm factors are significant.*

Throughout all the simulations and consecutive analyses, a statistically significant difference has been identified between the authentication protocols and their interactions with increased number of challenges. For each of our hypotheses the difference of α 0.5 and $p - value$ resulted on accepting only the alternative hypotheses in each case.

5. Threat Model

Our NIZKP protocol provides mitigation from existing threat vectors both in current proposal state and the features introduced in its future developments. We identify a class of attacks prominent to our case with an explanation on both the potential attack vectors and mitigations in place as part of NIZKP's

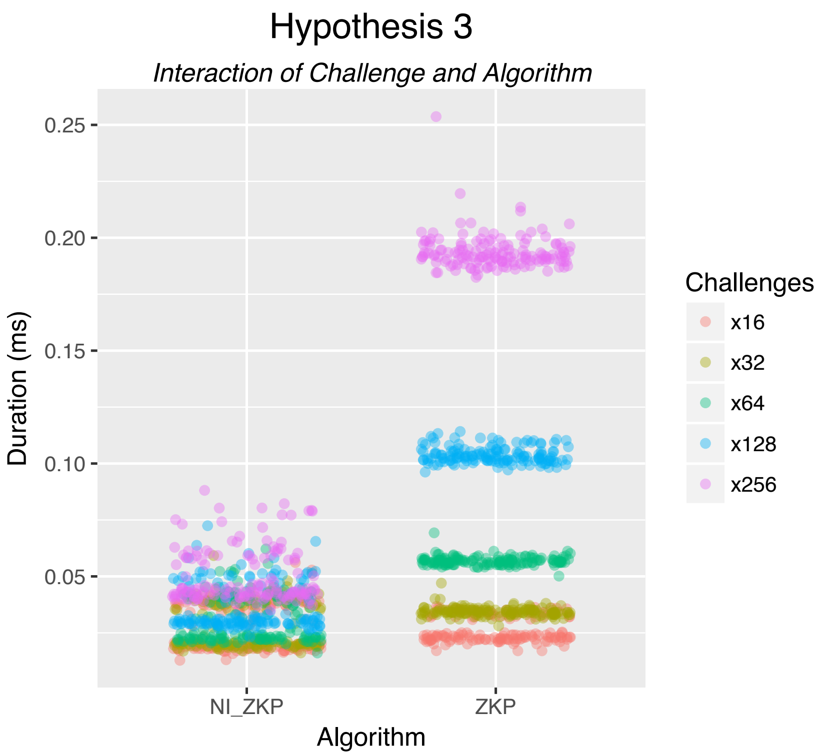

Figure 10: Effect of Interaction of Algorithm and Challenges.

interactions. Authentication requests should not be routed through the IoT device, especially when the gateway acts as the registration authority for the network. If such routing is permitted getaway bypass attacks might be possible. Since hash trees are used to construct the authentication chain, our protocol can form the basis for future meshed mutual authentication schemes in IoT networks. Threat mitigation on the client side against a stolen V attack has been mitigated in our scheme as there is no password transmitted. Therefore, password guessing is infeasible against NIZKP as the way our challenge is calculated renders this attack vector unusable.

Although an adversary could sample the authentication challenge for multiple client authentication requests against a uniquely identified UUID, there are no values stored at any stage in the authentication process. In the scenario of node impersonation and replay attacks, an adversary may be able to impersonate a sensor node and by accessing secret values such as the temporal client UUID, he or she might be able to re-create the challenge. The proposed auditing and logging of authentication requests from a client against UUIDs and the published root node hash for each session, prevents an adversary from replaying the challenge or injecting a challenge packet based on rebuild sample values. When nodes, sensors are deployed in unattended environments, they become susceptible to node capture attacks. In a node capture attack, any sensor or entity with the network can act as an adversary whereby they can capture, re-program and re-deploy a node within the target network [46]. This attack can lead to significant security and privacy risks within the environment. Without proper network monitoring procedures in place, device absence as a result of a physical capture can not be noticed [47], [48]. This type of attacks can render further attacks such as Sybil and selective forwarding possible.

In cases that the same hash function is used for both leaves and branch nodes in the Merkle tree structure it would be possible to generate collisions or even second preimages with arbitrary values. If for example m is a message longer than the segment size of the hash tree, $h_{internal}$ be the internal hashing function and the leaf hash function h_{leaf}, then the hashing value of m can be calculated as: $h(m) = h_{internal}(h_{leaf}(m_0)||h_{leaf}(m_1)$, where m_0, m_1 are the different segments of m. If a m' exist such that $m' \neq m$ and $h(m') = h_{leaf}(m') = h_{leaf}(h_{leaf}(m0)||h_{leaf}(m1))$ if $h_{leaf} = h_{internal}$ then $h_{(m')} = h_{(m)}$ that can constitute a second preimage attack.

Authors in [49] have introduced several preimage attacks against the dithered variants of the Merkle-Damgard mode of operation. Further attacks have been recorded in the literature with regards to the application of Merkle trees in several applications such as bitcoin and Blockchain networks [50]. Often, these applications do not distinguish between inner nodes and leaf nodes, thus the length of the tree is often implicitly given by the number of corresponding transactions inside the network. An exhaustive discussion on these attacks is outside the scope of our work. We have also identified that adversaries can extract configuration information and impersonate legitimate participants during the authentication process. All pre-cautions must be taken to ensure the configuration between the gateway and the sensor is encrypted, leading to an unforgeable Merkle tree generation. Mitigation of this risk has been considered in our future work where device specific fingerprinting is utilised in the provision of uniquely identifiable information as part of NIZKP's operation.

6. Conclusion and future work

This work seeks to articulate the design, development and the preliminary quantitative study of a novel authentication protocol based on NIZKP. Our NIZKP protocol has been designed specifically to offer performance and quality enhancements for the authentication challenges in resource constraint networks with clear identification of existing security threats. An experiment was designed to compare the performance of our protocol that utilises NIZKP based on Merkle trees against a traditional ZKP approach using graph isomorphism. We developed a set of statistical experiments to validate hypotheses based on key metrics on observation data produced by our simulations. Throughout the analysis, we rejected all null hypotheses namely the number of authentication challenges issued by the protocol and effects on performance, interactions and effects on performance, and protocols' operation and their effect on performance. We have identified that the construction of the Merkle Tree grants further investigation including the processing of the packet challenge, node recall and tree traversal as fundamental components in the creation of more resource-efficient algorithms. Also, although SHA256 has been used as the de-facto algorithm in our work, its effectiveness in resource contraint environments must be examined further. Further improvements might be possible utilising hashes such as LOCHA.

Although the hash values used in our challenge pack at time restricted, further evaluation is needed on the data protection processes introduced during the calculation of these hashes. Our simulations use randomly generated data values to seed the nodes during the Merkle tree creation. We are currently seeking optimal solutions to obtain the seeding data for the data nodes in a cryptographically resistant manner while verifying the creation of the Merkle tree.

References

[1] K. Thomas, A. Moscicki, D. Margolis, V. Paxson, E. Bursztein, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, Data Breaches, Phishing, or Malware?, Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '17 (2017) 1421–1434.

[2] H. S. Ahmed, Wireless Sensor Network for Medical Applications 11 (1) (2015) 49–59.

[3] L. Larkey, L. Bettencourt, A. Hagberg, In-situ data quality assurance for environmental applications of wireless . . . , Los Alamos Natl. . . . V (2006) 1–13.

[4] M. Srbinovska, C. Gavrovski, V. Dimcev, A. Krkoleva, V. Borozan, Environmental parameters monitoring in precision agriculture using wireless sensor networks, J. Clean. Prod. 88 (2015) 297–307.

[5] B. Pannetier, J. Dezert, G. Sella, Multiple target tracking with wireless sensor network for ground battlefield surveillance, in: 17th International Conference on Information Fusion (FUSION), 2014, pp. 1–8.

[6] C. P. Kruger, G. P. Hancke, Implementing the Internet of Things vision in industrial wireless sensor networks, 2014 12th IEEE Int. Conf. Ind. Informatics (2014) 627–632.

[7] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3599–3609. doi:10.1109/TII.2017.2773666.

[8] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K. R. Choo, A robust and energy efficient authentication protocol for industrial internet of things, IEEE Internet of Things Journal 5 (3) (2018) 1606–1615. doi:10.1109/JIOT.2017.2787800.

[9] A.-S. K. Pathan, Security of self-organizing networks : MANET, WSN, WMN, VANET, Auerbach Pub, 2011.

[10] R. Rajagopalan, P. K. Varshney, Data-aggregation techniques in sensor networks: A survey, IEEE Commun. Surv. Tutorials 8 (4) (2006) 48–63.

[11] G. Padmavathi, D. Shanmugapriya, A survey of attacks, security mechanisms and challenges in wireless sensor networks, CoRR abs/0909.0576. arXiv:0909.0576.
URL http://arxiv.org/abs/0909.0576

[12] Q. Yaseen, M. Aldwairi, Y. Jararweh, M. Al-Ayyoub, B. Gupta, Collusion attacks mitigation in internet of things: a fog based model, Multimedia Tools and Applications 77 (14) (2018) 18249–18268. doi:10.1007/s11042-017-5288-3.
URL https://doi.org/10.1007/s11042-017-5288-3

[13] A. G. Dinker, t. y. v. n. p. k. d. I. m. V. Sharma, booktitle=2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).

[14] Yih-Chun Hu, A. Perrig, D. B. Johnson, Wormhole attacks in wireless networks, IEEE Journal on Selected Areas in Communications 24 (2) (2006) 370–380. doi:10.1109/JSAC.2005.861394.

[15] S. Souaidi, T. Kenaza, B. Djamaa, M. Aldwairi, Dynamic clustering for iot key management in hostile application area, in: O. Demigha, B. Djamaa, A. Amamra (Eds.), Advances in Computing Systems and Applications, Springer International Publishing, Cham, 2019, pp. 48–56.

[16] IEEE, IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011) : IEEE Standard for Low-Rate Wireless Networks. (2016).
URL http://ieeexplore.ieee.org/document/7460875/

[17] P. Sarkar, A. Saha, Security enhanced communication in wireless sensor networks using reed-muller codes and partially balanced incomplete block designs, J. Converg. 2 (1) (2011) 23–30.

[18] X. Liao, Z. Qin, L. Ding, Data embedding in digital images using critical functions, Signal Processing: Image Communication 58 (2017) 146 – 156. doi:https://doi.org/10.1016/j.image.2017.07.006.
URL http://www.sciencedirect.com/science/article/pii/S0923596517301364

[19] R. k. Dwivedi, P. Sharma, R. Kumar, A scheme for detection of high transmission power based wormhole attack in wsn, in: 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, pp. 1–6. doi:10.1109/UPCON.2018.8596853.

[20] S. H. Rose, T. Jayasree, Detection of jamming attack using timestamp for wsn, Ad Hoc Networks 91 (2019) 101874. doi:https://doi.org/10.1016/j.adhoc.2019.101874.
URL http://www.sciencedirect.com/science/article/pii/S157087051830667X

[21] Y. Gao, H. Ao, Z. Feng, W. Zhou, S. Hu, W. Tang, Mobile network security and privacy in wsn, Procedia Computer Science 129 (2018) 324 – 330, 2017 INTERNATIONAL CONFERENCE ON IDENTIFICATION,INFORMATION AND KNOWLEDGEIN THE INTERNET OF

THINGS. doi:https://doi.org/10.1016/j.procs.2018.03.083. URL http://www.sciencedirect.com/science/article/pii/S187705091830320X

[22] N. Khernane, M. Potop-Butucaru, C. Chaudet, Banzkp: A secure authentication scheme using zero knowledge proof for wbans, in: 2016 13th International Conference on New Technologies for Distributed Systems (NOTERE), 2016, pp. 1–6. doi:10.1109/NOTERE.2016.7745828.

[23] L. Ma, Y. Ge, Y. Zhu, Tinyzkp: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks, Wirel. Pers. Commun. 77 (2) (2014) 1077–1090. doi:10.1007/s11277-013-1555-4. URL http://dx.doi.org/10.1007/s11277-013-1555-4

[24] K. H. M. Wong, Y. Zheng, J. Cao, S. Wang, A dynamic user authentication scheme for wireless sensor networks, in: IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), Vol. 1, 2006, p. 8 pp.

[25] M. S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment, Ad Hoc Networks 36 (2016) 152 – 176.

[26] B. Vaidya, D. Makrakis, H. Mouftah, Two-factor mutual authentication with key agreement in wireless sensor networks, Secur. Commun. NETWORKS 9 (2012) 171–183.

[27] M. Blum, A. De Santis, S. Micali, G. Persiano, Noninteractive zero-knowledge, SIAM J. Comput. 20 (6) (1991) 1084–1118. doi:10.1137/0220068. URL https://doi.org/10.1137/0220068

[28] U. Feige, A. Fiat, A. Shamir, Zero-knowledge proofs of identity, J. Cryptol. 1 (2) (1988) 77–94.

[29] C. C. C. H. J.-y. Q. C.-L. L. Yi-Ning Liu, Wei Guo, A Robust Electronic Voting Scheme Against Side Channel Attack, J. Inf. Sci. Eng. 32 (2016) 1471–1486.

[30] S. S. Nagamuthu Krishnan, P. Srinivasan, A QOS parameter based solution for black hole denial of service attack in wireless sensor networks, Indian J. Sci. Technol. 9 (38).

[31] R. Henry, I. Goldberg, Formalizing anonymous blacklisting systems, Proc. - IEEE Symp. Secur. Priv. 2 (2011) 81–95.

[32] S. Naik, N. Shekokar, Conservation of energy in wireless sensor network by preventing denial of sleep attack, Procedia Comput. Sci. 45 (C) (2015) 370–379.

[33] F. Martín-Fernández, P. Caballero-Gil, C. Caballero-Gil, Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things, Sensors 16 (12) (2016) 75.

[34] H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, An efficient Merkle-tree-based authentication scheme for smart grid, IEEE Syst. J. 8 (2) (2014) 655–663.

[35] B. Ederov, Merkle Tree Traversal Techniques (April) (2007) 42.

[36] L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L. Ni, J. Ma, Pseudo trust: Zero-knowledge authentication in anonymous p2ps, IEEE Transactions on Parallel and Distributed Systems 19 (10) (2008) 1325–1337. `doi:10.1109/TPDS.2008.15`.

[37] S. Grzonkowski, Sedici: An authentication service taking advantage of zero-knowledge proofs, in: Financial Cryptography, 2010.

[38] N. Bitansky, R. Canetti, A. Chiesa, E. Tromer, From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again, in: Proceedings of the 3rd Innovations in Theoretical Computer

Science Conference, ITCS '12, ACM, New York, NY, USA, 2012, pp. 326–349. doi:10.1145/2090236.2090263.
URL http://doi.acm.org/10.1145/2090236.2090263

[39] Q. Xu, R. Zheng, W. Saad, Z. Han, Device Fingerprinting in Wireless Networks: Challenges and Opportunities 18 (1) (2015) 94–104.

[40] P. Jiang, F. Guo, K. Liang, J. Lai, Q. Wen, Searchain: Blockchain-based private keyword search in decentralized storage, Future Generation Computer Systemsdoi:https://doi.org/10.1016/j.future.2017.08.036.
URL http://www.sciencedirect.com/science/article/pii/S0167739X17318630

[41] A. Beydemir, Soğukpinar, Lightweight zero knowledge authentication for internet of things, in: 2017 International Conference on Computer Science and Engineering (UBMK), 2017, pp. 360–365. doi:10.1109/UBMK.2017.8093410.

[42] I. . Chuang, B. Guo, J. Tsai, Y. Kuo, Multi-graph zero-knowledge-based authentication system in internet of things, in: 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–6. doi:10.1109/ICC.2017.7996820.

[43] I. Chatzigiannakis, A. Pyrgelis, P. G. Spirakis, Y. C. Stamatiou, Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 715–720. doi:10.1109/MASS.2011.77.

[44] A. L. Al-Bajjari, L. Yuan, Research of web security model based on zero knowledge protocol, in: 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2016, pp. 68–71. doi:10.1109/ICSESS.2016.7883017.

[45] P. Bratley, B. Fox, L. Schrage, A Guide to Simulation, Springer Science Business Media, 2012.

[46] S. Agrawal, M. L. Das, J. Lopez, Detection of node capture attack in wireless sensor networks, IEEE Systems Journal 13 (1) (2019) 238–247. doi:10.1109/JSYST.2018.2863229.

[47] M. Aldwairi, M. A. Alshboul, A. Seyam, Characterizing realistic signature-based intrusion detection benchmarks, in: Proceedings of the 6th International Conference on Information Technology: IoT and Smart City, ICIT 2018, ACM, New York, NY, USA, 2018, pp. 97–103. doi:10.1145/3301551.3301591.
URL http://doi.acm.org/10.1145/3301551.3301591

[48] M. Aldwairi, A. Y. Hamzah, M. Jarrah, Multiplzw: A novel multiple pattern matching search in lzw-compressed data, Computer Communications 145 (2019) 126 – 136. doi:https://doi.org/10.1016/j.comcom.2019.06.011.
URL http://www.sciencedirect.com/science/article/pii/S014036641930458X

[49] E. Andreeva, C. Bouillaguet, P.-A. Fouque, J. J. Hoch, J. Kelsey, A. Shamir, S. Zimmer, Second preimage attacks on dithered hash functions, in: Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings, Vol. 4965 of Lecture Notes in Computer Science, Springer, 2008, pp. 270–288. doi:10.1007/978-3-540-78967-3_16.

[50] RESERVED, Trusted Merkle Tree Depth for Safe Tx Inclusion Proofs Without a Soft Fork, https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-12842, [Online; accessed 2-November-2018] (2018).