CAKE: Hybrides Gruppen-Schlüssel-Management Verfahren

Peter Hillmann, Marcus Knüpfer und Gabi Dreo Rodosek[1]

Abstract: Mit zunehmender Vernetzung von Systemen gibt es immer mehr Teilnehmer, die innerhalb einer Gruppe über ungesicherte Kommunikationskanäle vertrauliche Informationen austauschen. Um den Zugriff auf diese Daten durch Dritte zu verhindern, ist das Verschlüsseln dieser unumgänglich. Dazu nutzen die Gruppenteilnehmer einen gemeinsamen Schlüssel, der gesichert zu verteilen ist. Gerade im Bereich von MANETs bilden die begrenzten Ressourcen hinsichtlich der Rechen- und Übertragungskapazität sowie die dynamisch ändernde Gruppenzusammensetzung besondere Herausforderungen. Zur Koordinierung und Verteilung wird in der vorliegenden Arbeit ein neuartiges, hybrides Gruppen-Schlüssel-Management Verfahren vorgestellt, welches zentral organisiert ist und strikten Sicherheitsanforderungen genügt. Durch einen hybriden Ansatz werden die Vorteile der existierenden Protokolle kombiniert, mit dem Ziel den Berechnungs- und Kommunikationsaufwand zu verringern. Es wird gezeigt, dass sich das Verfahren für ändernde MANET-Gruppen besser eignet als die bestehenden. Darüber hinaus lässt sich das Verfahren auch in weiteren Anwendungsgebieten, wie kabelgebundenen Weitverkehrsnetzen einsetzen. Der Gruppenschlüssel ist dabei für beliebige Dienste anwendbar.

Keywords: Sichere Kommunikation, Ad hoc Netz, MANET, GKMP, Schlüsselmanagement

1 Einleitung

Für den Austausch von Daten innerhalb einer Gruppe existieren zur Verwaltung der Gruppenschlüssel sogenannte Gruppen-Schlüssel-Management (GKM) Verfahren. Diese übernehmen den sicheren und effizienten Austausch der Schlüssel, welche zur Kommunikation innerhalb einer Gruppe genutzt werden. Alle Teilnehmer einer Gruppe besitzen dazu den gleichen symmetrischen Schlüssel, wodurch die Informationen nur ein einziges Mal für die Teilnehmer der Gruppe zu verschlüsseln sind. Für welchen Dienst der gemeinsame Gruppenschlüssel eingesetzt wird, ist schlussendlich jedoch freigestellt.

Verschiedene Anwendungsbereiche haben spezifische Anforderungen an die Eigenschaften eines GKM Verfahrens, wodurch sich kein Verfahren als allgemeingültiger Lösungsansatz anwenden lässt. In der vorliegenden Arbeit wird ein GKM Verfahren vorgestellt, welches an eine Umgebung mit begrenzter Kommunikationsbandbreite und geringer Rechenleistung der Gruppenteilnehmer angepasst ist. Die vorrangige Motivation liegt in der Verbesserung der Effizienz gegenüber derzeitigen Verfahren, sodass im Netz mehr Bandbreite für die Nutzdaten zur Verfügung steht. Auf Basis des klassischen *Group Key Management Protocol* (GKMP), des *Secure Lock* (SL) und der *Local Key Hierarchy* (LKH) wird ein hybrides Verfahren zum GKM entwickelt.

[1] Universität der Bundeswehr München, Lehrstuhl für Kommunikationssysteme und Netzsicherheit, Werner-Heisenberg-Weg 39, D-85577 Neubiberg, {peter.hillmann, marcus.knuepfer. gabi.dreo}@unibw.de

Abschnitt 2 erläutert zunächst ein Szenario, um daraus Anforderungen abzuleiten. Anschließend wird in Abschnitt 3 auf den Stand der Technik eingegangen und in Abschnitt 4 das neue Verfahren vorgestellt. Eine Bewertung der Sicherheitsanforderungen befindet sich in Abschnitt 5. Abschließend werden die Ergebnisse der Arbeit zusammengefasst.

2 Szenario und Anforderungen

Als Anwendungsbeispiel dient ein militärisches Szenario im Bereich der sogenannten mobilen Ad-hoc-Netze (MANET). Hierbei bewegen sich mehrere Teilnehmer in einem Gelände und tauschen währenddessen mittels Funkkommunikation Nachrichten aus. In Abb. 1 sind verschiedene Zustände dargestellt, aus denen sich die typischen Gruppenoperationen ableiten lassen. Die jeweils verschiedenfarbigen Kreise entsprechen dem Kommunikationsradius bzw. dem Schlüsselbereich der jeweiligen Gruppe. Die 8-12 Teilnehmer werden durch die taktischen Zeichen dargestellt. Im Zustand 1 befindet sich eine Gruppe A auf dem Weg eine andere Gruppe B zu unterstützen. Zur gesicherten Kommunikation beider Gruppen müssen diese in einen gemeinsamen Schlüsselbereich eintreten (Gruppenverschmelzung). Im Zustand 2 ist dargestellt, wie ein einzelner Späher die vereinigte Gruppe erreicht und in den gemeinsamen Schlüsselbereich eintritt (Eintritt). Dieser berichtet von nicht identifizierten Personen, welche in der Nähe gesichtet wurden. Infolgedessen trennt sich Gruppe A aus dem Verbund (Gruppenteilung) und bewegt sich in Richtung der aufgeklärten Personen, dargestellt durch Zustand 3. Im letzten Zustand 4 wird aus Gruppe A ein Melder zur Materialübergabe in den rückwärtigen Raum geschickt, welcher somit die Gruppe verlässt (Austritt).
Weitere zivile Anwendungsbeispiele sind Multicast-Datenübertragungen im Bereich vom Video on Demand oder dynamische Projektteams in der Forschung.

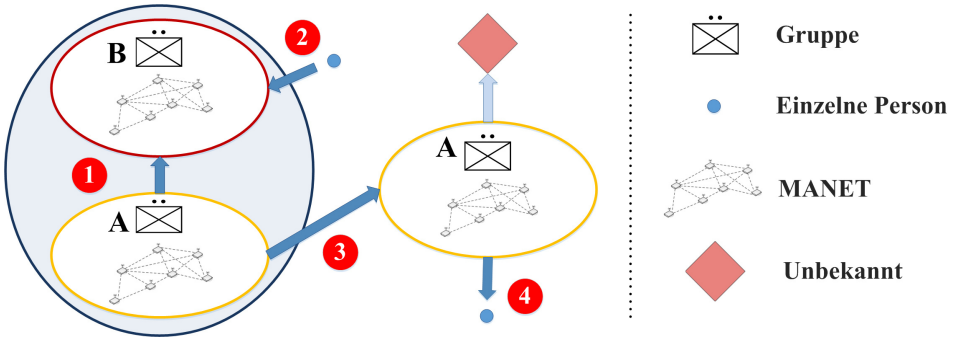

Abb. 1: Verschiedene Operationen bei der verschlüsselten Gruppenkommunikation

Für die sichere Übermittlung von Nachrichten ist ein Kryptosystem notwendig, welches sich in die Rahmen des MANET einfügt. Hierbei werden folgende Anforderungen an die Sicherheit gestellt [Bu13]:

- *Forward Secrecy:* Austretenden Teilnehmern soll es nicht mehr möglich sein, weiterhin empfangene Nachrichten entschlüsseln zu können.
- *Backward Secrecy:* Eintretenden Teilnehmern soll es nicht möglich sein, im Vorfeld empfangene Nachrichten im Nachhinein entschlüsseln zu können.

- *Kollisionsfreiheit:* Eine unerlaubte Vorgehensweise einer Teilmenge von Teilnehmern führt nicht zum Schaden eines einzelnen Gruppenteilnehmers.
- *Schlüsselunabhängigkeit / Folgenlosigkeit:* Die Kenntnis eines Schlüssels ermöglicht keine Schlussfolgerung auf weitere Schlüssel.

Im Zusammenhang mit dem Szenario ergeben sich daraus die folgenden Anforderungen an die Gruppenoperationen, welche durch ein modernes GKM Verfahren abzudecken sind, ohne dabei die Sicherheitsanforderungen zu missachten:

- *Einzel- und Mehrfach-Eintritt:* Ein oder mehrere Teilnehmer treten in eine bestehende Gruppe ein. (Beachtung der Backward Secrecy)
- *Einzel- und Mehrfach-Austritt:* Ein oder mehrere Gruppenmitglieder treten aus der Gruppe aus. (Beachtung der Forward Secrecy)
- *Re-Keying:* Die Aktualisierung des Gruppenschlüssels muss über eine effiziente Vorgehensweise möglich sein.
- *Gruppenverschmelzung:* Mehreren Gruppen ist durch Re-Keying ein gemeinsamer Schlüssel effizient bereitzustellen. (Beachtung der Backward Secrecy)
- *Gruppenteilung:* Eine Gruppe teilt sich in mehrere Teilgruppen auf. (Beachtung der Forward Secrecy)

Zur Entlastung der Teilnehmer werden die Schlüssel zentral von einer Basis-Station mit mehr Leistung generiert und über eine hierarchische Struktur verteilt. Dadurch verlagert sich der Rechenaufwand für die Schlüsselgenerierung zu einer Instanz. Jeder Teilnehmer besitzt über das MANET bzw. über einen Satelliten-Link eine Kommunikationsverbindung zu der zentralen und vertrauenswürdigen Basis-Station. Hierbei werden folgende Anforderungen gestellt:

- Verschlüsselte und gesicherte Nachrichtenübermittlung, da diese insbesondere bei Verwendung von Funkkommunikation abhörbar ist.
- Eine geringe verfügbare Bandbreite bedingt kleine Datenpakete und eine geringe Anzahl an Nachrichten.
- Die geringe Rechenleistung der mobilen Funkgeräte ist zu berücksichtigen.
- Der Overhead durch das Management der Gruppenschlüssel ist gering zu halten.

3 Stand der Technik

Die verschiedenen GKM Verfahren lassen sich in drei Hauptkategorien einteilen, welche wiederum aus verschiedenen Unterkategorien bestehen [CS08, Ra00]. Bei zentralisierten Verfahren erfolgt die Vergabe des Gruppenschlüssels durch eine zentrale Kontrollstelle. Demgegenüber stehen dezentralisierte Verfahren, bei denen die Schlüsselgenerierung und -verteilung durch wechselnde Instanzen möglich ist. Darüber hinaus gibt es noch Verfahren mit verteilten Schlüsselvereinbarungen, wobei eine Aufteilung in Untergruppen stattfindet, welche voneinander unabhängige Gruppenschlüssel nutzen.

Gemäß der Forderung nach einem zentralisierten Verfahren wird nur diese Kategorie vertiefend betrachtet. Hierbei gibt es die folgenden drei Unterkategorien [CS08]:

- *Paarweise Schlüssel:* Übermittlung des Gruppenschlüssels durch die zentrale Instanz mittels individueller Teilnehmerkommunikation
- *Broadcast Geheimnis:* Übertragung des Gruppenschlüssels mittels Broadcast anstelle individueller Verbindungen
- *Hierarchische Schlüssel:* Einordnung der Teilnehmer in eine Baumstruktur mit entsprechenden kryptografischen Schlüsseln zur Verteilung der Gruppenschlüssel

Der bekannteste Vertreter der paarweisen Schlüssel ist das GKMP [HM97]. Bei diesem Protokoll speichert und teilt sich der zentrale Server einen geheimen Schlüssel mit jedem Gruppenmitglied. Dieser wird *Key-Encryption-Key* (KEK) genannt. Zur Verteilung des Gruppenschlüssels sendet der Server jedem Teilnehmer einzeln diesen Schlüssel individuell mit dem jeweiligen KEK überschlüsselt, was zu einem hohen Aufwand führt. Durch die mehrfache Datenübertragung von der zentralen Instanz zu den einzelnen Teilnehmern, sowohl bei der Erstellung einer Gruppe als auch bei jeder Veränderung der Gruppenkonstellation, sind viele Nachrichten notwendig. Dadurch entsteht eine erhebliche Belastung für den Server und der ohnehin geringen Netzkapazität des MANET.

Demgegenüber steht das Broadcast-basierte Verfahren SL [CC89, AM08], welches dem Server ermöglicht komplette *Re-Keying* Prozesse mit jeweils einer einzigen Broadcast-Nachricht durchzuführen. Es basiert auf dem *Chinese Remainder Theorem* (CRT) [XCD12], welches zur Erzeugung einer Verschlüsselung die Eigenschaften der Kongruenz ausnutzt. Jedoch ist die Berechnung des CRT im Vergleich zum GKMP noch aufwendiger, sodass dies für Endgeräte im Bereich von MANETs mit geringer Rechenleistung nur in begrenztem Umfang durchführbar ist.

Das alternative Verfahren LKH [Li12, Sa14] gehört zu den hierarchischen GKM Verfahren. Die Schlüssel und damit die Gruppenteilnehmer werden hierbei in einem für jede Gruppe eigens angelegten Binärbaum gepflegt. Jeder Knoten im Baum repräsentiert einen KEK, welcher den darunter liegenden Teilnehmern bekannt ist. Durch den Aufbau der Baumstruktur entsteht ein erhöhter Aufwand hinsichtlich der Verwaltung der vielen inneren Knoten sowie der Berechnung und Verteilung zugehöriger Schlüssel was nur im Fall eines Austritts einen mäßigen Vorteil bietet. Da es nicht bei jeder Verwendung zu dieser Operation kommt, ist dies unnötiger Aufwand. Zudem sind im Vergleich zum SL mehrere Nachrichten beim Austritt zu versenden, was zu einer erhöhten Netzlast führt.

4 CAKE - Hybrides Gruppen-Schlüssel-Management Verfahren

Für die gestellten Anforderungen im Bereich von MANETs wird folgendes Konzept zum Management der Gruppenschlüssel vorgeschlagen. Das neu entwickelte Verfahren *Central Authorized Key Extension* (CAKE) nutzt dazu einzelne Bestandteile der zuvor genannten Verfahren und kombiniert diese zu einem integrierten hybriden System. Gemäß den Anforderungen des Szenarios ist die Schlüsselverwaltung bei CAKE zentral organisiert.

Hierzu existiert eine autorisierte und vertrauenswürdige Instanz (AI), welche die Generierung, Verwaltung und Verteilung der Schlüssel übernimmt sowie notwendige Berechnungen durchführt. Jeder Teilnehmer N_i meldet sich am System an, indem dieser mit der AI ein privates Schlüsselpaar (KEK_i) aushandelt. Weiterhin generiert jeder Teilnehmer eine Primzahl m_i für ein CRT System. Mit diesen beiden Geheimnissen KEK_i und m_i ist ein Teilnehmer bei der AI im System CAKE angemeldet.

Neben den individuellen und persönlichen Schlüsseln umfasst CAKE noch einen *Group-Transmission-Encryption-Key* (GTEK), welcher für die eigentliche Kommunikation in der Gruppe verwendet wird. Hierzu muss jeder Teilnehmer einer Gruppe in Besitz dieses Schlüssels sein. Zusätzlich existiert ein *Group-Key-Encryption-Key* (GKEK). Dieser wird bei Bedarf zur Überschlüsselung des GTEK verwendet, sodass dieser gesichert an alle Kommunikationsteilnehmer verteilt werden kann. Zur Überschlüsselung werden die beiden Schlüssel GTEK und GKEK bitweise mit XOR verrechnet. Die Verwendung der XOR Operation bietet informationstheoretische Sicherheit gemäß dem One-Time-Pad.

4.1 Initiale Erzeugung einer Gruppe und des ersten GTEK

Bei der Erzeugung einer Gruppe generiert die AI zufällig einen GTEK und einen GKEK. Diese sind an alle Gruppenteilnehmer für die gesicherte Kommunikationsgruppe zu verteilen. Dazu berechnet die AI analog zum SL Verfahren initial ein CRT System und übermittelt die Daten mittels einer Broadcast-Nachricht. Hierbei werden von allen Teilnehmern der spezifizierten Gruppe die Werte m_i mit in die Berechnung des sogenannten Locks *MX* einbezogen. Ein Teilnehmer N_i kann das Lock gemäß dessen Prinzip nur auflösen, wenn der spezifische Wert m_i in der Berechnung enthalten ist. Die Empfänger der Nachricht erhalten als Ergebnis des CRT Systems den Schlüssel GKEK. Der Schlüssel GTEK wird durch bitweises XOR mit dem GKEK überschlüsselt und in einer weiteren Broadcast-Nachricht übermittelt. Folgende Bestandteile sind zur initialen Erzeugung einer Gruppe bei allen Gruppenmitgliedern notwendig: $\{GKEK\}_{Lock\,MX}$, $\{GTEK\}_{GKEK}$

Die Teilnehmer der Gruppe müssen zuerst das Lock *MX* auflösen, um den GKEK zu erhalten. Anschließend lässt sich der Schlüssel GTEK ermitteln. Somit haben alle Teilnehmer die Kenntnis über die einheitlichen Gruppenschlüssel GTEK und GKEK. Bei Bedarf kann die Nachricht entsprechend digital mit dem Zertifikat der AI signiert werden.

4.2 Eintritt von neuen Teilnehmern in eine Gruppe

Wenn nach der Gruppenerzeugung ein neuer Teilnehmer N_{i+1} an der gesicherten Gruppenkommunikation teilnehmen möchte, muss dieser zuerst die initialen Prozesse mit der AI durchlaufen. Dieser meldet sich dazu bei der AI des Systems CAKE an und tauscht die Schlüsselinformationen (KEK_{i+1}, m_{i+1}) aus. Anschließend wird ein Re-Keying für die bestehende Gruppe durchgeführt. Dazu generiert die AI den Schlüssel $GTEK_{neu}$ und $GKEK_{neu}$. Diese werden bitweise mit XOR unter Zuhilfenahme des gehashten $GKEK_{aktuell}$

überschlüsselt. Die entstandene Nachricht wird an alle bisherigen Gruppenteilnehmer gesendet. Für den neuen Teilnehmer N_{i+1} wird der $GTEK_{neu}$ und $GKEK_{neu}$ mit dem privaten Schlüssel KEK_{i+1} verschlüsselt und separat übertragen. Durch entsprechend zeitsynchrones Umschalten vom $GTEK_{aktuell}$ auf $GTEK_{neu}$ können alle Teilnehmer gesichert miteinander kommunizieren.

Bei einem Masseneintritt von mehreren neuen Teilnehmern in eine Gruppe wird äquivalent zum Eintreten eines neuen Teilnehmers verfahren. Alternativ lassen sich die neuen Gruppenteilnehmer über ein CRT zusammenfassen, sodass nur eine Nachricht für alle neuen Teilnehmer notwendig ist. Somit sind beim Eintreten eines neuen Teilnehmers in eine Gruppe zwei einfache Berechnungen (XOR und Verschlüsselung gemäß Verfahren) sowie zwei Broadcast-Nachrichten notwendig. Beim Eintreten mehrerer neuer Teilnehmer sind durch die Verwendung eines CRT Systems ebenfalls nur zwei Nachrichten notwendig. Bei der Verschmelzung bestehender Gruppen wird jeweils ein Re-Keying auf Grundlage der bestehenden GKEKs der Gruppen durchgeführt, wodurch nur entsprechend der Anzahl der zu verschmelzenden Gruppen Nachrichten notwendig sind.

4.3 Austritt von Teilnehmern aus eine Gruppe

Beim Austritt eines Teilnehmers aus einer Gruppe können die bestehenden GTEK und GKEK nicht genutzt werden, da der austretende Teilnehmer diese entschlüsseln kann. Eine erneute Initialisierung der Gruppe mittels CRT System ist aufgrund des Berechnungsaufwandes ebenso nicht praktikabel. Zur Reduktion des Aufwandes wird in CAKE ein verkleinertes CRT System angewendet und eine ternäre Baumstruktur eingesetzt, welche durch die AI verwaltet wird.

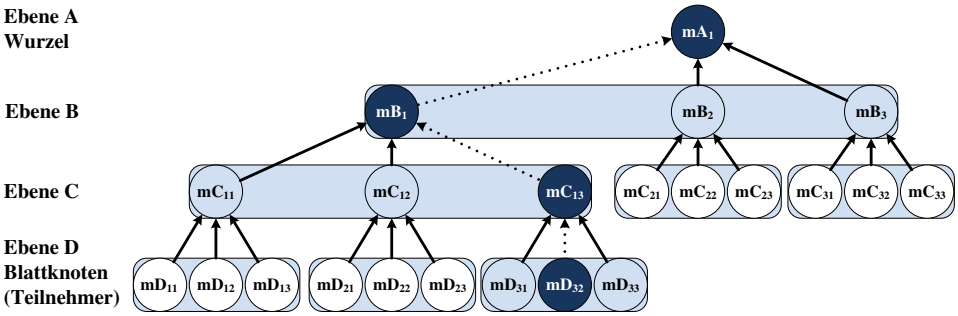

Abb. 2: Ternäre Baumstruktur zur Verwaltung der Schlüssel und zur Reduktion des Berechnungsaufwandes beim Austritt.

Abb. 2 verdeutlicht diese Baumstruktur, welche in Ebenen, beginnend mit A an der Wurzel, eingeteilt ist. Wie bei LKH entsprechen die Teilnehmer einer Gruppe mit deren m_i den Blattknoten des Baumes. Darüber hinaus entsprechen die Knoten weiteren KEKs, welche den darunter liegenden Teilnehmern bekannt sein müssen. Die Bezeichnung *mX* eines Knoten definiert ein spezifisches *m* für das CRT System, wobei das *X* die Ebene darstellt. Alle auf dem Pfad von der Wurzel zum Teilnehmer liegenden Schlüssel *m* müssen dem entsprechenden Teilnehmer bekannt sein, welche nur bei Bedarf initialisiert werden. Die

entsprechenden *mX* der Knoten entlang eines Pfades werden durch mehrere, kleine CRT Systeme von unten nach oben im Baum aufgebaut, sodass die Menge der Nachrichten gering gehalten wird. Baumstrukturen mit mehreren Unterknoten sind für größere Gruppen durch die flachere Struktur besser geeignet als Binärbäume. Mit jeweils maximal drei Unterknoten reduziert sich die Menge der zu berechnenden Locks für Gruppengrößen bis 81 Teilnehmer vorteilhaft. Im Bereich der betrachteten militärischen MANETs (selten mehr als 60 Teilnehmer) bietet sich somit die ternäre Baumstruktur an. Vorteilhaft ist ebenso, dass sich die Informationen zu den *mX* zu beliebigen Zeitpunkten bei geringer Netzbelastung aufbauen und versenden lassen.

Beim Austritt eines Teilnehmers wird der entsprechende Pfad von der Wurzel zum Blatt in der Baumstruktur markiert (in Abb. 2: Knoten mD_{32}, dunkel markiert). Alle auf dem markierten Pfad liegenden Schlüssel *mX* werden bei der folgenden CRT Berechnung nicht mit einbezogen. Für die Berechnung des notwendigen Locks *MX* des verkleinerten CRT Systems werden die jeweils neben einem markierten Knoten auf gleicher Ebene befindlichen *mX* verwendet (in Abb. 2: schraffiert gekennzeichnet). Diese stellen die Menge der in der Gruppe verbleibenden Teilnehmer dar, mittels welchen das neue Lock *MX* gebildet wird. Diese Menge hat wesentlich weniger Elemente als bei der Initialisierung der Gruppe und folglich ist der Rechenaufwand geringer. Die in die Berechnung einbezogenen Werte reduzieren sich von n-1 auf ($ln\ n_{max}$ / ln 3) * 2 (in Abb. 2: von 14 auf 6). Dabei entspricht n_{max} der Anzahl von Blättern bei einem vollbesetzten Baum. Somit ist nur eine Nachricht an die verbleibenden Teilnehmer zu senden. Die unter einem Teilbaum liegenden Teilnehmer können das Lock *MX* auflösen, da diesen der jeweilige *mX* auf dem Pfad bekannt ist. Nach Abschluss des Austrittes sind die *mX* auf dem dunkel markierten Pfad zu erneuern, indem die AI diese den Teilnehmern mitteilt. Bei einem Austritt mehrerer Teilnehmer oder einer Gruppenteilung sind vor der Berechnung in der Baumstruktur entsprechend mehrere Pfade zu markieren.

4.4 Re-Keying für eine Gruppe

Für das Re-Keying des GTEK einer Gruppe existieren zwei Möglichkeiten. In der ersten Variante generiert die AI oder ein beliebiger Gruppenteilnehmer neue $GTEK_{neu}$ und $GKEK_{neu}$. Diese werden jeweils mit dem gehashten $GKEK_{aktuell}$ bitweise XOR verschlüsselt und digital signiert. Das entstandene Datagramm wird anschließend an alle Gruppenteilnehmer per Broadcast verschickt. Durch die Spezifikation eines Zeitpunktes kann die Gruppe synchron auf den $GTEK_{neu}$ umschalten. Die zweite Variante sieht die Nutzung der individuellen Schlüssel der Teilnehmer bzw. des CRT Systems vor. Dabei verfährt die AI entsprechend des Konzeptes der initialen Erzeugung einer Gruppe bzw. des ersten GTEK.

4.5 Vergleichende Bewertung von CAKE

Tabelle 1 stellt das neu entwickelte Protokoll CAKE vergleichend gegenüber den bisherigen Verfahren dar. Es ist ersichtlich, dass CAKE bei der Erzeugung von Gruppen einen

vergleichbar hohen Berechnungsaufwand wie SL hat. Allerdings ergibt sich für die Erweiterung und Verkleinerung der Gruppe ein geringer Berechnungsaufwand im Vergleich zu allen anderen Systemen. In Abb. 3 ist der Vergleich des Berechnungsaufwandes anschaulich dargestellt, wobei für die Aufwandsbetrachtung entsprechend der Berechnungskomplexität die XOR-Operation mit Wertigkeit 1, die symmetrische Verschlüsselungsoperation mit Wertigkeit 2 und die CRT-Berechnung mit Wertigkeit 3 vereinfacht abgebildet sind. Darüber hinaus ist bei CAKE die Anzahl der Nachrichten gering, wodurch die Netzlast niedrig bleibt. Abb. 4 stellt diesen funktionalen Zusammenhang dar. Diese Vorteile des Systems werden durch einen Mehrbedarf an Schlüsseln und Speicherplatz für die Schlüssel erreicht. Da Schlüssel nur eine geringe Größe haben, ist dieser Nachteil vernachlässigbar. Diese Eigenschaften des Systems CAKE sind insbesondere im Bereich von gesicherter Funkkommunikation bei MANETs als vorteilhaft zu bewerten. Zusammenfassend entsteht durch den integrierten hybriden Ansatz ein Verfahren, welches den Berechnungsaufwand und die Anzahl zu übertragender Nachrichten minimiert.

Tab. 1: Gegenüberstellung verschiedener Gruppen-Schlüssel-Management Protokolle.

	Berechnungsaufwand			Nachrichtenanzahl			Bandbreite in L			Speicherbedarf in L	
	Initial	Eintritt	Austritt	Initial	Eintritt	Austritt	Initial	Eintritt	Austritt	Server	Teilnehmer
GKMP	nE	2E	(n-1)E	n	n+1	n-1	n	n+1	n-1	n	1+G
SL	nC	(n+1)C	(n-1)C	1			1			nG	2G
LKH	$2log_2$nE			$2log_2$n			$2log_2$n			(2n-1)*G	(2n-1)*G
CAKE	nC	XOR+E	2E *ln* n/*ln* 3	2			2			n+(1+3^k)*G	(2+k)*G+1

n ... Anzahl der Gruppenteilnehmer
G ... Anzahl der Gruppen eines Teilnehmers
C ... Teilnehmer der CRT Lock Berechnung
L ... Länge des Schlüssels
E ... Symmetrische Verschlüsselungsoperation
k ... Höhe des verwalteten Baumes

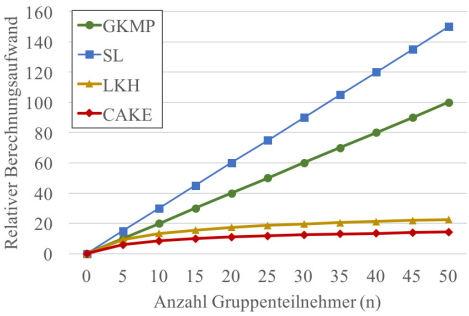

Abb. 3: Vergleich des durchschnittlichen Berechnungsaufwandes der betrachteten Verfahren

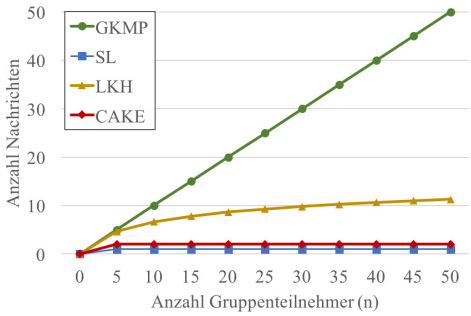

Abb. 4: Vergleich der durchschnittlichen Nachrichtenanzahl der betrachteten Verfahren

5 Bewertung der Sicherheit und Erläuterung des Designs

Im Folgenden wird die Sicherheit von CAKE hinsichtlich der in Abschnitt 2 erwähnten Sicherheitsanforderungen bewertet. Darüber hinaus erfolgen Erläuterungen zur Konstruktion des Sicherheitsdesigns.

Unterteilung in GKEK und GTEK
Ein separater GKEK zur Verbreitung eines neuen GTEK ist notwendig, da die Nutzung des aktuellen $GTEK_{aktuell}$ als $GKEK_{aktuell}$ bei bitweisen XOR dazu führt, dass der neue Teilnehmer die alten Nachrichten entschlüsseln könnte. Durch Anwendung von XOR auf die abgefangene Nachricht mit $GTEK_{neu}$ ergibt sich $GTEK_{aktuell}$. Dies wird durch den Einsatz eines separaten GKEK verhindert.

Forward- und Backward Secrecy
Backward Secrecy wird hierbei durch die Kombination der beiden Schlüssel GKEK und GTEK sowie dem CRT erreicht. Bei Eintritt von Teilnehmern werden die Schlüssel entsprechend neu generiert. Das CRT System beruht auf der Verwendung der persönlichen KEK der berechtigten Teilnehmer, sodass es für andere Teilnehmer nicht zu entschlüsseln ist. Bei Austritt von Teilnehmern oder einer Gruppenteilung findet der beschriebene Prozess zum Schlüsselwechsel statt, welcher die Forward Secrecy sicherstellt. Durch die Verwendung der ternären Baumstruktur in Verbindung mit dem reduzierten CRT System (Zwischenknoten im Baum) werden der GTEK und der GKEK in einem solchen Szenario mit vergleichbar geringem Berechnungsaufwand neu bestimmt und verteilt.

Im Zusammenhang mit dem gestellten Szenario ist die Sicherheit des allgemeinen Re-Keying-Prozesses durch die Nutzung des GKEK gewährleistet und der Aufwand gering gehalten. Im Falle von sogenannten “Man in the Middle“ Angriffen, bei denen einzelne Nachrichten abgefangen und verfälscht bzw. nicht weitergeleitet werden, bleibt der Nachrichteninhalt somit trotzdem geheim.

Schlüsselunabhängigkeit / Folgenlosigkeit
Durch den Einsatz einer XOR-Verknüpfung, welche nachweislich nicht zu dechiffrieren ist (vgl. [MM13], [BL12]), beim Verschlüsseln der GTEK und GKEK ist es auch nach Abfangen eines der benutzen Schlüssel nicht möglich auf den ursprünglichen zu schließen. Die voneinander unabhängige Erzeugung der einzelnen Schlüssel und die Verwendung von Hashfunktionen gewährleistet die Folgenlosigkeit.

Kollisionsfreiheit
Bei der Verschlüsselung von Nachrichten wird, gängigerweise unter Zuhilfenahme von Zufall, bei jeder Durchführung ein einzigartiger Key erstellt. Dies verhindert Rückschlüsse von bereits abgefangenen bzw. dechiffrierten Schlüsseln auf neu erlangte. Ein von nicht vertrauenswürdigen Teilnehmern initiierter Re-Keying Prozess wird durch die Struktur des Verfahrens verhindert, da dies nur mit Insiderwissen von der bestehenden Gruppe und der AI durchgeführt werden kann. Ferner ist eine Autorisierung durch die AI bei Eintritt eines Teilnehmers in das Kommunikationsnetz erforderlich. In Verbindung mit dem Einsatz von digitalen Signaturen ist die benötigte Sicherheit gewährleistet.

6 Zusammenfassung

Im Bereich von MANETs ist zur verschlüsselten Kommunikation die Verwendung von Ressourceneffizienten Verfahren essentiell. Mit CAKE wird in der vorliegenden Arbeit ein entsprechend den Anforderungen genügendes GKM Verfahren vorgestellt und mit dem

Stand der Technik verglichen. CAKE bietet die Möglichkeit bei geringem Berechnungsaufwand und einer niedrigen Belastung des Netzes, Schlüssel innerhalb einer Gruppe auszutauschen und effizient auf dynamische Veränderungen der Gruppe zu reagieren. Dabei ermöglicht CAKE stets eine vertrauliche Verteilung der Schlüssel und die Einhaltung der Anforderungen hinsichtlich Backward und Forward Secrecy. Auf Basis der aufgezeigten Betrachtungen ist es im nächsten Schritt notwendig, das entwickelte Verfahren praktisch im MANET einzusetzen.

Danksagung

Wir danken Sandro Passarelli für die Diskussionen und Anregung zum praktischen Szenario. Die Arbeit wurde durch das siebente Rahmenprogramm des Exzellenznetzwerkes (ICT-318488) über das Projekt FLAMINGO durch die europäische Kommission gefördert.

Literaturverzeichnis

[AM08] Antosh, C. J.; Mullins, B. E.: The Scalability of Secure Lock. In: IEEE International Performance, Computing, and Communications Conference. Jgg. 27, S. 507–512, 2008.

[BL12] Borowski, M.; Lesniewicz, M.: Modern usage of "old" one-time pad. In: Military Communications and Information Systems Conference (MCC). S. 1–5, 2012.

[Bu13] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Katalog, M 2.46 Geeignetes Schlüsselmanagement. 2013.

[CC89] Chiou, Guang-Huei; Chen, Wen-Tsuen: Secure broadcasting using the secure lock. IEEE Transactions on Software Engineering, 15(8):929–934, 1989.

[CS08] Challal, Yacine; Seba, Hamida: Group Key Management Protocols: A Novel Taxonomy. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2(10):3620 – 3633, 2008.

[HM97] Harney, H.; Muckenhirn, C.: Group Key Management Protocol (GKMP) Specification. Bericht 2093, Internet Engineering Task Force, 1997.

[Li12] Liu, Zenghui; Lai, Yingxu; Ren, Xubo; Bu, Shupo: An Efficient LKH Tree Balancing Algorithm for Group Key Management. In: Proceedings of the International Conference on Control Engineering and Communication Technology (ICCECT). Jgg. 10. IEEE Computer Society, S. 1003–1005, 2012.

[MM13] Matt, C.; Maurer, U.: The one-time pad revisited. In: IEEE International Symposium on Information Theory Proceedings (ISIT). Jgg. 11, S. 2706–2710, 2013.

[Ra00] Rafaeli, Sandro: A Decentralised Architecture for Group Key Management. Bericht, Lancaster University, 2000.

[Sa14] Sakamoto, N.: An efficient structure for LKH key tree on secure multicast communications. In: IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). Jgg. 15, S. 1–7, 2014.

[XCD12] Xu, Guoyu; Chen, Xingyuan; Du, Xuehui: Chinese Remainder Theorem based DTN group key management. In: IEEE International Communication Technology (ICCT). Jgg. 14, S. 779–783, 2012.